SIEMENS

# Tecnologia industrial de comutação

## SIRIUS Safety Integrated

Manual de Aplicativos

Answers for industry.

SIEMENS

# Tecnologia industrial de comutação

# SIRIUS
# Safety Integrated Application Manual

Manual de Aplicativos




10/2014

A5E33346617003A/RS-AA/001

# Informações jurídicas

## Conceito de aviso

Este manual contém instruções que devem ser observadas para sua própria segurança e também para evitar danos materiais. As instruções que servem para sua própria segurança são sinalizadas por um símbolo de alerta, as instruções que se referem apenas à danos materiais não são acompanhadas deste símbolo de alerta. Dependendo do nível de perigo, as advertências são apresentadas como segue, em ordem decrescente de gravidade.

| ⚠PERIGO |
| --- |
| significa que **haverá** caso de morte ou lesões graves, caso as medidas de segurança correspondentes não forem tomadas. |

| ⚠AVISO |
| --- |
| significa que **poderá haver** caso de morte ou lesões graves, caso as medidas de segurança correspondentes não forem tomadas. |

| ⚠CUIDADO |
| --- |
| indica um perigo iminente que pode resultar em lesões leves, caso as medidas de segurança correspondentes não forem tomadas. |

| ATENÇÃO |
| --- |
| significa que podem ocorrer danos materiais, caso as medidas de segurança correspondentes não forem tomadas. |

Ao aparecerem vários níveis de perigo, sempre será utilizada a advertência de nível mais alto de gravidade. Quando é apresentada uma advertência acompanhada de um símbolo de alerta relativamente a danos pessoais, esta mesma também pode vir adicionada de uma advertência relativa a danos materiais.

## Pessoal qualificado

O produto/sistema, ao qual esta documentação se refere, só pode ser manuseado por **pessoal qualificado** para a respectiva definição de tarefas e respeitando a documentação correspondente a esta definição de tarefas, em especial as indicações de segurança e avisos apresentados. Graças à sua formação e experiência, o pessoal qualificado é capaz de reconhecer os riscos do manuseamento destes produtos/sistemas e de evitar possíveis perigos.

## Utilização dos produtos Siemens em conformidade com as especificações

Tenha atenção ao seguinte:

| ⚠AVISO |
| --- |
| Os produtos da Siemens só podem ser utilizados para as aplicações especificadas no catálogo e na respetiva documentação técnica. Se forem utilizados produtos e componentes de outros fornecedores, estes têm de ser recomendados ou autorizados pela Siemens. Para garantir um funcionamento em segurança e correto dos produtos é essencial proceder corretamente ao transporte, armazenamento, posicionamento, instalação, montagem, colocação em funcionamento, operação e manutenção. Devem-se respeitar as condições ambiente autorizadas e observar as indicações nas respetivas documentações. |

## Marcas

Todas denominações marcadas pelo símbolo de propriedade autoral ® são marcas registradas da Siemens AG. As demais denominações nesta publicação podem ser marcas em que os direitos de proprietário podem ser violados, quando usadas em próprio benefício, por terceiros.

## Exclusão de responsabilidade

Nós revisamos o conteúdo desta documentação quanto a sua coerência com o hardware e o software descritos. Mesmo assim ainda podem existir diferenças e nós não podemos garantir a total conformidade. As informações contidas neste documento são revisadas regularmente e as correções necessárias estarão presentes na próxima edição.

Siemens AG
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
ALEMANHA

3ZX1012-0SK11-1AG1
℗ 10/2014 Sujeito a alterações

# Índice remissivo

# 1 Introdução

## Objetivo da documentação

Esta documentação fornece uma visão dos requisitos básicos de segurança da indústria transformadora. A documentação mostra exemplos de circuitos simples com base nos produtos SIRIUS Safety Integrated, relativos a funções de segurança das seguintes áreas de aplicação:

- Paralisar em caso de emergência
- Monitoramento da porta de proteção
- Monitoramento das rotações/paralisação
- Monitoramento de áreas de perigo abertas
- Operação segura
- Combinações típicas de funções de segurança

No seguimento dos exemplos de circuitos simples, encontra informações de fundo detalhadas relativas a prescrições e normas, bem como sobre a especificação e o design de peças relevantes à segurança dos comandos.

## Grupo-alvo

Esta documentação contém informações para os seguintes grupos-alvo:

- Decisores
- Tecnólogos
- Projetistas

## Conhecimentos necessários

Para compreender esta documentação são necessários conhecimentos básicos gerais nas seguintes áreas:

- Tecnologia de comutação de baixa tensão
- Tecnologia de comutação digital
- Técnica de automação

## Garantia e responsabilidade

**Indicação**

Os exemplos de aplicativos não são vinculativos e não pretendem ser exaustivos relativamente à configuração e equipamento, bem como a quaisquer eventualidades. Os exemplos de aplicativos não representam soluções personalizadas, devendo apenas servir de suporte de ajuda para tarefas típicas. O próprio usuário é responsável pela operação correta dos produtos descritos. Estes exemplos de aplicativos não o isentam da responsabilidade pelo manuseamento seguro durante a aplicação, instalação, operação e manutenção. Reservamo-nos o direito de efetuar alterações nestes exemplos de aplicativos a qualquer momento e sem aviso prévio. Se existirem divergências entre as propostas apresentadas nestes exemplos de aplicativos e outras publicações da Siemens, como p. ex. catálogos, o prioritário é o conteúdo da outra documentação.

Não assumimos qualquer responsabilidade pelas informações contidas neste documento.

Isentamo-nos de qualquer responsabilidade, independentemente da causa legal, por danos causados pela utilização dos exemplos, indicações, programas, dados sobre a execução de projetos e de potência, descritos nestes exemplos de aplicativos.

A exclusão não se aplica a situações que, por dolo ou negligência, ponham em causa a vida, a integridade física ou a saúde, nem a outros danos resultantes de má conduta ou negligência grosseira.

É proibida a transmissão ou reprodução destes exemplos de aplicativos, ou extratos dos mesmos, desde que tal não tenha sido expressamente autorizado pela Siemens Industry Sector.

## Histórico

Até à data, já foram publicadas as seguintes versões desta documentação. As alterações aplicam-se à versão de produto anterior:

| Emissão | Observação/Alteração |
|---|---|
| 09/2013 | Primeira versão |
| 10/2013 | Pequenos melhoramentos a nível da redação, reparação de links com defeito |
| 03/2014 | Integração de exemplos complementares de aplicativos, alargamento e correção de conteúdos |
| 09/2014 | Aditamentos e correções de conteúdos |

# Engenharia de segurança geral 2

## 2.1 Conceitos básicos

### Redundância

Na redundância são utilizados vários componentes para a mesma função, de forma que se um dos componentes estiver a funcionar incorretamente é substituído pelo outro ou pelos outros componentes. A montagem redundante permite reduzir a probabilidade de uma falha de funcionamento devido a componentes individuais com defeito. Este requisito é necessário para se obter um Safety Integrity Level SILCL 3 segundo IEC 62061, SIL 3 segundo IEC 61508 e PL e segundo ISO 13849-1 (em determinadas circunstâncias, também é necessário para SIL 2 / PL d).

A forma mais simples para a redundância é a de dois canais. A montagem de dois canais garante que a função de segurança continua assegurada caso um circuito falhe. Na montagem de um sistema redundante, a detecção e reação dos subsistemas também têm de ser realizadas com dois canais.

---

**Indicação**

Todos os aparelhos SIRIUS-Safety, que cumprem a SILCL 3 segundo IEC 62061, SIL 3 segundo IEC 61508 e PL e segundo ISO 13849-1, têm uma estrutura redundante tanto em relação à lógica interna como em relação aos circuitos de saída.

---

### Detecção de circuitos transversais

A detecção de circuitos transversais é uma função de diagnóstico de uma unidade de avaliação, na qual também são detectados curtos-circuitos ou circuitos cruzados entre dois canais de entrada (circuitos de sensores), no caso de uma detecção ou leitura de dois canais. Um circuito cruzado pode surgir, por exemplo, devido ao esmagamento de um cabo revestido, o que, no caso de aparelhos sem detecção de circuitos transversais, pode ter como consequência que, p. ex., um circuito de parada de emergência de dois canais não acione qualquer desligamento mesmo quando apenas um contato de interrupção tem falha (segundo erro).

### Circuito de liberação

Um circuito de liberação disponibiliza um sinal de saída relativo à segurança. Geralmente, os circuitos de liberação atuam para o exterior como contatos de estabelecimento (funcional mas é sempre considerada a abertura segura). Um circuito de liberação individual, que esteja montado internamente de forma redundante no dispositivo de comutação de segurança, pode ser utilizado para SIL 3 / PL e. Observação: Os circuitos de corrente de ativação também podem ser utilizados para finalidades de aviso.

## Circuito de retorno

O circuito de retorno serve para monitorar os atuadores ativados (p. ex. relé ou contator de carga) com contatos de ação positiva ou contatos espelho. Os circuitos de liberação só podem ser ativados com o circuito de retorno fechado.

Na utilização de um caminho de desativação redundante, é necessário avaliar o circuito de retorno dos dois atuadores. Para o efeito, estes também podem ser ligados em série.

## Arranque automático

No arranque automático, o aparelho é iniciado sem consentimento manual, mas somente após a verificação da imagem de entrada e o teste positivo da unidade de avaliação. Esta função também é designada como funcionamento dinâmico e não é permitida para equipamentos de parada de emergência. As instalações de proteção para zonas de perigo intransitáveis (p. ex. interruptor de posição, grade de luz, esteira sensível a pressão) podem trabalhar com o arranque automático, caso não advenha daí qualquer perigo.

## Arranque vigiado

No arranque vigiado, a máquina é iniciada mediante a ligação do botão de arranque, após a verificação da imagem de entrada e após o teste positivo da unidade de avaliação. O arranque vigiado avalia a mudança de sinal do botão de arranque. Desta forma, o comando do botão de arranque não pode ser enganado. Para PL e (ISO 13849-1) e SIL 3 (IEC 62061) é necessário utilizar o arranque vigiado em caso de parada de emergência. Para outros sensores/funções de segurança, a necessidade de uma ordem de arranque vigiado depende da avaliação de riscos.

## Arranque manual

No arranque manual, o aparelho é iniciado mediante a ligação do botão de arranque, após a verificação da imagem de entrada e após o teste positivo do dispositivo de comutação de segurança. No arranque manual, o funcionamento correto do botão de arranque não é monitorado, é suficiente um flanco positivo do botão de arranque para iniciar.

---

**Indicação**

O arranque manual não é permitido para equipamentos de parada de emergência.

---

## Operação com duas mãos/sincronismo

O acionamento síncrono de sensores é uma forma especial de simultaneidade dos sensores. Neste caso, não é apenas necessário que os contatos dos sensores 1 e 2 sejam comutados em conjunto para o estado fechado "num período à escolha", mas é igualmente necessário que os contatos dos sensores sejam fechados num período de 0,5 s. A solicitação do sincronismo dos sensores ocorre especialmente nos comandos de duas mãos em prensas. Neste caso, pretende-se assegurar que a prensa só fica ativa quando os sensores são acionados ao mesmo tempo com as duas mãos. Desta forma é minimizado o risco de o operador ativar inadvertidamente a prensa.

## Abertura positiva

Os interruptores de abertura positiva estão estruturados de um modo, que quando o interruptor é ligado ocorre uma abertura inevitável dos contatos. Os contatos soldados são quebrados com a ligação (EN 60947-5-1).

## Contatos de ação positiva

Num componente com contatos de manobra positiva está garantido, que os contatos de interrupção e de estabelecimento nunca estão fechados ao mesmo tempo (EN 60947-5-1).

## Contatos espelho

Um contato espelho é um contato de interrupção, que garante que não pode estar fechado em simultâneo com um contato principal (EN 60947-4-1).

## 2.2 Generalidades

Neste capítulo encontra informações gerais e transversais sobre o tema da engenharia de segurança.

Os detalhes sobre prescrições e normas, bem como sobre a especificação e o design de peças relevantes à segurança dos comandos, encontram-se no fim deste manual.

### 2.2.1 Objetivo da engenharia de segurança

O objetivo da engenharia de segurança é o de reduzir ao máximo o perigo para o homem e para o ambiente através de medidas construtivas e dispositivos técnicos, sem restringir a produção industrial, a utilização de máquinas ou o fabrico de produtos químicos, para além do estritamente necessário. As regulamentações acordadas internacionalmente devem proporcionar a proteção do homem e do ambiente na mesma medida a todos os países, e ao mesmo tempo evitar distorções da concorrência devido a diferentes requisitos de segurança no comércio internacional.

### 2.2.2 Leis locais

Um dado importante para os fabricantes de máquinas e instaladores de equipamento é o fato de se aplicarem sempre as leis e regras do local onde a máquina ou instalação será operada. Como por exemplo, o comando de uma máquina que deverá ser operada nos EUA tem de preencher os requisitos locais, mesmo que o fabricante da máquina seja proveniente da UE. Mesmo quando os conceitos técnicos, que visam garantir a segurança, estão sujeitos a legalidades técnicas, é igualmente importante verificar se existem disposições legislativas com determinadas especificações ou restrições.

## 2.2.3 Segurança funcional

A segurança é indissociável do ponto de vista do bem a proteger. Uma vez que as causas dos perigos e, consequentemente, as medidas técnicas para a sua prevenção, podem ser muito distintas umas das outras, é feita a distinção entre diferentes tipos de segurança, p. ex., mediante a indicação da respectiva causa de potenciais perigos. Assim, fala-se de "segurança elétrica", quando é necessário referir a proteção contra perigos inerentes à energia elétrica, ou de "segurança funcional", quando a segurança depende do funcionamento correto.

Para que a segurança funcional de uma máquina ou de uma instalação seja alcançada, é necessário que as peças relevantes à segurança das instalações de proteção e dos equipamentos de comando funcionem corretamente e que, em caso de falha, se comportem de forma a assegurar que a instalação permanece ou é colocada num estado seguro.

Para o efeito, é necessário utilizar uma tecnologia especialmente qualificada que preencha os requisitos descritos nas normas pertinentes. Os requisitos para se alcançar a segurança funcional, baseiam-se nos seguintes objetivos fundamentais:

- Evitação de erros sistemáticos
- Controle dos erros sistemáticos
- Controlo de erros ou falhas acidentais

A medida para a segurança funcional alcançada, é a probabilidade de falhas perigosas, a tolerância de erros e a qualidade, com a qual deve ser assegurada a isenção de erros sistemáticos. Tal é expresso nas normas por meio de diferentes conceitos:

- Em IEC 62061: "Safety Integrity Level" (SIL)
- Em ISO 13849-1: "Performance Level" (PL)

## 2.2.4 Objetivo das normas

Da responsabilidade que fabricante e usuário têm pela segurança dos dispositivos técnicos e produtos, resulta a exigência de tornar as instalações, máquinas e outro dispositivos técnicos tão seguros quanto o estado da tecnologia o permite. Para tal, o estado da tecnologia é descrito em normas pelos parceiros econômicos, relativamente a todos os aspetos relevantes para a segurança. Mediante o cumprimento das respectivas normas relevantes é possível assegurar que o estado da tecnologia foi alcançado e que o instalador de um equipamento ou o fabricante de uma máquina ou de um aparelho cumpriu o seu dever de prudência.

Os detalhes relativos às prescrições e normas encontram-se no capítulo Prescrições e normas (Página 123).

---

**Indicação**

**Sem pretensão de exaustividade**

As normas, diretivas e leis referidas neste manual são uma opção de transmitir objetivos e princípios essenciais. A lista não pretende ser exaustiva.

---

### 2.2.5 Funções relacionadas com a segurança

As funções relacionadas com a segurança abrangem funções clássicas e outras mais complexas.

**Funções clássicas:**

- Paralisação
- Ações em caso de emergência
- Prevenção de partida inadvertida

**Funções mais complexas:**

- Bloqueios em função do estado
- Limitação da velocidade
- Limitação da posição
- Paralisação controlada
- Parada controlada, entre outros

### 2.2.6 Paralisação

#### Paralisação (categorias de parada da EN 60204-1)

Para paralisar uma máquina estão definidas em EN 60204-1 (VDE 0113 Parte 1) três categorias de parada, que descrevem o processo de comando para a paralisação, independentemente de uma situação de emergência:

| Categoria de parada | Significado |
|---|---|
| 0 | Categoria 0 de parada devido ao desligamento imediato da energia para os elementos de acionamento da máquina |
| 1 | Categoria 1 de paralisação; a alimentação de energia só é interrompida após a paralisação. |
| 2 | Categoria 2 de paralisação, na qual a alimentação de energia é mantida durante a paralisação. |

**Indicação**

Com o desligamento só é interrompida a alimentação de energia que pode provocar um movimento. Não há isenção de tensão.

### 2.2.7 Ação em caso de emergência

EN 60204-1 / 11.98 determinou e definiu as seguintes ações possíveis para casos de emergência (EN 60204-1 Anexo D). Os termos entre parêntesis correspondem à versão do projeto final da edição 5.0 de IEC 60204-1.

Uma ação em caso de emergência implica, individualmente ou em combinação, o seguinte:

- Paralisar em caso de emergência (parada de emergência)
- Arranque de emergência (arranque de emergência)
- Parada de emergência (parada de emergência)
- Ativação de emergência (Ativação de emergência)

Segundo EN 60204-1 e ISO 13850 estas funções só podem ser ativadas por ação humana consciente. Por conseguinte, será abordado apenas a "Parada de emergência" e o "Paralisar em caso de emergência". O último corresponde plenamente ao termo com o mesmo nome da diretiva sobre máquinas UE (ingl. Emergency Stop). Por razões de simplificação, serão utilizados de seguida os termos alternativos Parada de emergência e Desligar em caso de emergência.

### 2.2.8 Parada de emergência

Uma ação em caso de emergência que se destina a desligar a energia elétrica de toda uma instalação ou de uma parte da instalação, caso exista risco de choque elétrico ou um outro risco de natureza elétrica (de EN 60204-1 Anexo D).

Os aspetos funcionais da parada de emergência estão definidos em IEC 60364-4-46 (idêntico a HD 384-4-46 e VDE 0100 Parte 460). Uma parada de emergência deve ser prevista, quando

- Uma proteção contra contato direto (p. ex. com linhas condutoras, corpos de anéis coletores, aparelhos de chaveamento em áreas de operação elétrica) só é alcançada através de distância ou de obstáculos;
- Existe a possibilidade de haver outros perigos ou danos devido a energia elétrica.

Para além disso, é referido em 9.2.5.4.3 de EN 60204-1: Uma parada de emergência é alcançada com o desligamento da máquina da alimentação, com o seguimento de uma parada da categoria 0.

Se a parada de categoria 0 não for permitida para uma máquina, poderá ser necessário providenciar uma outra proteção, p. ex., contra contato direto, de forma a tornar desnecessária uma parada de emergência.

Isso significa, que a parada de emergência deve ser utilizada onde a análise de risco indica um perigo devido a tensão/energia elétrica, sendo requerido um desligamento imediato e abrangente da tensão elétrica.

### 2.2.9 Parada de emergência

Uma ação em caso de emergência que se destina a parar um processo ou um movimento que originaria perigo (de EN 60204-1 Anexo D). Para além disso, é referido em 9.2.5.4.2 de EN 60204-1:

Adicionalmente aos requisitos para a parada (ver 9.2.5.3 de EN 60204-1), aplicam-se os seguintes requisitos para desligar em caso de emergência:

- Tem de ter prioridade sobre todas as outras funções e operações em todos os modos de funcionamento
- A energia para os elementos de acionamento das máquinas que possam originar um estado que acarreta perigo ou estados que acarretam perigo, tem de ser desligada tão depressa quanto possível sem que sejam gerados outros perigos (p. ex. através de dispositivos de parada mecânicos que não necessitem de alimentação externa, através de frenagem contra-corrente na categoria de parada 1).
- O reset não pode originar um rearranque.

O paralisar em caso de emergência tem de atuar como parada da categoria 0 ou como parada da categoria 1 (ver 9.2.2 de EN 60204-1). A categoria para paralisar em caso de emergência tem de ser definida em função da avaliação de riscos para a máquina.

Os aparelhos para a paralisação em caso de emergência têm de estar disponíveis em todos os postos de comando, bem como em todos os locais onde possa ser necessário efetuar uma paralisação em caso de emergência.

Para preencher os objetivos de proteção da EN 60204-1, aplicam-se os seguintes requisitos:

- No caso de uma ligação dos contatos, mesmo que o acionamento seja curto, é obrigatório que o aparelho de comando encaixe.
- Não pode ser possível que a máquina seja reiniciada a partir de um posto de comando principal afastado, sem que o perigo tenha sido previamente eliminado. O equipamento de parada de emergência tem de ser desbloqueado "no local" através de uma ação consciente.

### 2.2.10 Função de segurança

Uma função de segurança descreve a reação de uma máquina/instalação quando se verifica uma determinada ocorrência (p. ex. abertura de uma porta de proteção). A(s) função(ões) de segurança é/são executada(s) através de um sistema de comando relativo à segurança. Este é composto geralmente por três subsistemas: a detecção, a avaliação e a reação.

**Detecção (sensores):**

- O reconhecimento de um requisito de segurança, p. ex.: é acionada a parada de emergência ou um sensor para o monitoramento de uma área perigosa (grade de luz, scanner a laser, etc.).

**Avaliação (unidade de avaliação):**

- O reconhecimento de um requisito de segurança e a iniciação segura da reação, p. ex. desligamento dos circuitos de liberação.
- O monitoramento do funcionamento correto dos sistemas de sensores e de atuadores.
- A iniciação de uma reação quando são detectados erros.

**Reação (atuadores):**

- O desligamento do perigo de acordo com o comando de comutação da unidade de avaliação.

### 2.2.11 Seletor dos modos de funcionamento

As máquinas possuem frequentemente vários modos de funcionamento, que são comutados através de um seletor dos modos de funcionamento. Todas as máquinas têm de ser concebidas de forma a serem seguras em qualquer modo de funcionamento. Como o seletor dos modos de funcionamento comuta apenas entre modos de funcionamento seguros e protegidos por funções de segurança, este não tem de ser concebido de forma segura nem incluído no cálculo destas funções de segurança.

A própria seleção do modo operacional não pode ativar qualquer operação da máquina, essa tem de ser feita por um comando separado.

Se um modo de funcionamento requerer a supressão de uma função de segurança (p. ex. para um ajuste ou reparação), esta terá de ser substituída por uma outra função de segurança segundo EN 60204-1 capítulo 9.2.4.

Neste caso, é recomendável montar eletricamente o seletor dos modos de funcionamento de forma idêntica ao nível de segurança máximo de todos os modos de funcionamento. Neste caso, também não ocorre inclusão no cálculo das funções de segurança.

Para além disso, existem requisitos especiais para o seletor de modo de operação em determinados tipos de máquinas. Estes são referidos nas normas C para estes tipos de máquinas e têm de ser aplicados.

### Ver também

FAQs detalhadas sobre o tema Seleção do modo operacional (http://support.automation.siemens.com/WW/view/pt/89260861)

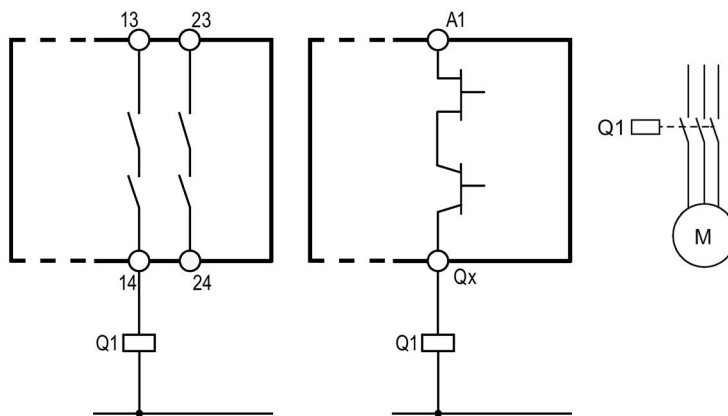
## 2.2.12 Conexão de atuadores

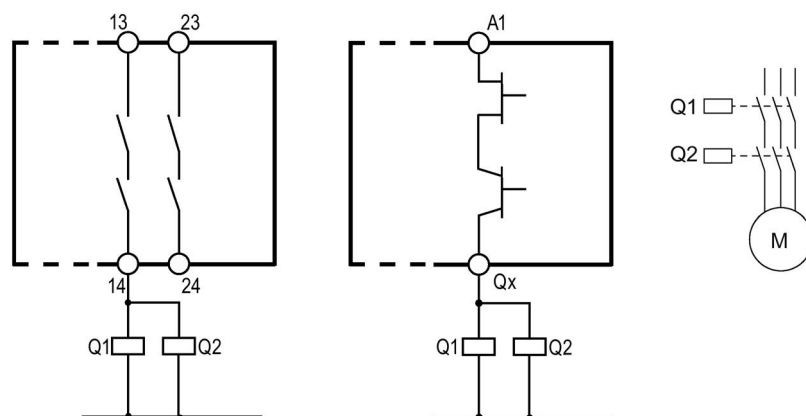
**Indicação**

Para alcançar os Performance Level/Safety Integrity Level referidos nos exemplos seguintes, é necessário monitorar os atuadores indicados no circuito de retorno do respectivo dispositivo de comutação de segurança.

**Indicação**

No caso de consumidores capacitivos e indutivos, recomendamos um circuito de proteção adequado. Dessa forma, as interferências eletromagnéticas podem ser suprimidas e a vida útil dos contatos aumentada.

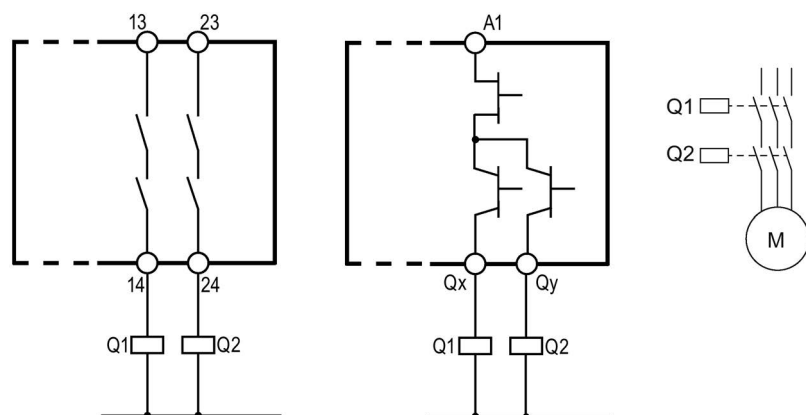
### Circuito de conexão de atuadores até PL c segundo ISO 13849-1 ou SILCL 1 segundo IEC 62061

Esquema 2-1 PL c segundo ISO 13849-1 ou SILCL 1 segundo IEC 62061

### Circuito de conexão de atuadores com instalação segura de cabos até PL e / cat. 4 segundo ISO 13849-1 ou exigência máxima SIL 3 segundo IEC 62061

Esquema 2-2 PL e segundo ISO 13849-1 ou SILCL 3 segundo IEC 62061

**⚠ AVISO**

PL e segundo ISO 13849-1 ou SILCL 3 segundo IEC 62061 só pode ser alcançado com cabeamento à prova de circuito transversal/à prova de circuito P das linhas de comando da saída dos dispositivos de comutação (p. ex. 14) para o relé/contator de comando (Q1 e Q2) (p. ex. como condutor isolado separado ou num duto para cabos próprio).

Em alguns dispositivos de comando pode haver limitação em relação ao nível de segurança alcançável, consulte a este respeito as indicações no manual do respectivo aparelho.

### Circuito de conexão de atuadores até PL e segundo ISO 13849-1 ou SILCL 3 segundo IEC 62061

Esquema 2-3 PL e segundo ISO 13849-1 ou SILCL 3 segundo IEC 62061

### 2.2.13 Ligação em série de sensores

#### Ligação em série de aparelhos de comando de parada de emergência

É possível realizar uma ligação em série de aparelhos de comando de parada de emergência até ao nível de segurança mais elevado SILCL 3 segundo IEC 62061, SIL 3 segundo IEC 61508 e PL e segundo ISO 13849-1, partindo-se do pressuposto que é sempre acionada apenas uma parada de emergência. Desta forma, é assegurada que os erros/defeitos podem ser detectados. Ver o capítulo "Paralisar em caso de emergência" - Introdução (Página 26).

#### Ligação em série de interruptores de posição

Por princípio, é possível ligar interruptores de posição em série, se for possível excluir a possibilidade de várias portas de proteção serem regularmente abertas em simultâneo (caso contrário, não é possível ocorrer uma detecção de erros)

Contudo, para o nível de segurança conforme SILCL 3 segundo IEC 62061, SIL 3 segundo IEC 61508 e PL e segundo ISO 13849-1 estes nunca podem ser ligados em série, devido ao fato de os erros perigosos terem de ser sempre detectados (independentemente do pessoal operador).

Ver o capítulo "Monitoramento da porta de proteção" - Introdução (Página 44).

#### Ligação em série de um aparelho de comando de parada de emergência e de um monitoramento da porta de proteção

Por princípio, é possível ligar um aparelho de comando de parada de emergência e um interruptor de posição em série, se for possível excluir a possibilidade de que ambos são abertos/acionados regularmente em simultâneo (caso contrário, não é possível ocorrer uma detecção de erros).
Contudo, para o nível de segurança conforme SILCL 3 segundo IEC 62061, SIL 3 segundo IEC 61508 e PL e segundo ISO 13849-1 estes nunca podem ser ligados em série, devido ao fato de os erros perigosos terem de ser sempre detectados (independentemente do pessoal operador).

Ver o capítulo "Combinações típicas de funções de segurança" - Introdução (Página 110).

# 3 Exemplos de aplicativos

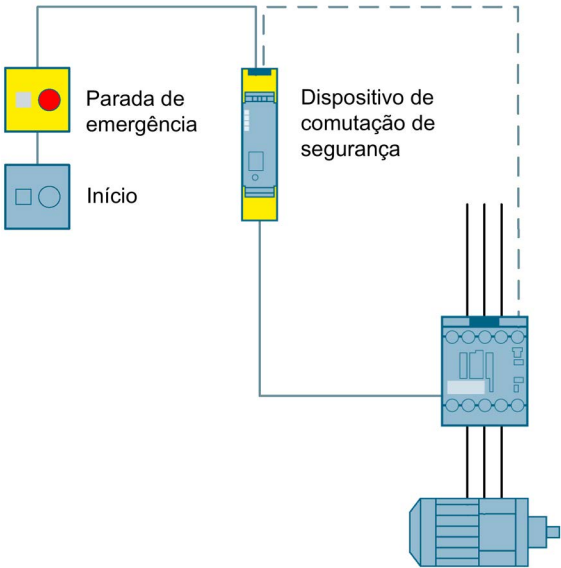
## 3.1 Introdução

Se existirem pessoas nas proximidades das máquinas (p. ex. na tecnologia de produção), estas têm de ser protegidas adequadamente através de equipamentos técnicos. Daí resulta uma multiplicidade de funções de segurança, que se destinam a servir este objetivo. A implementação de algumas das funções de segurança mais importantes será mostrada nos capítulos seguintes com base em exemplos de aplicativos de fácil compreensão. Os exemplos estão divididos segundo o tipo da função de segurança a realizar:

- Paralisar em caso de emergência
- Monitoramento da porta de proteção
- Monitoramento de áreas de perigo abertas
- Monitoramento das rotações/paralisação
- Operação segura
- Combinações típicas de funções de segurança

## Utilização dos exemplos de aplicativos

Os exemplos de aplicativos podem ser facilmente utilizados graças à sua estrutura uniforme. No início de cada exemplo, a aplicação é descrita de forma resumida. De seguida, é apresentada a estrutura da função de segurança com base em imagens sinóticas simples.

Os sinais dos sensores e o acionamento dos sistemas de atuadores são representados por linhas azuis, enquanto que o circuito de retorno para o monitoramento dos sistemas de atuadores é representado por uma linha tracejada.

Esquema 3-1 Apresentação do exemplo: Estrutura de uma função de segurança

O modo exato de funcionamento é explicado, tal como o nível de segurança máximo alcançável em SIL segundo IEC 62061 bem como em PL segundo ISO 13849-1.

**Apresentação do nível de segurança máximo alcançável**

| Aptidão para até SIL 1 / PL c | Aptidão para até SIL 2 / PL d | Aptidão para até SIL 3 / PL e |
|---|---|---|

Alguns exemplos de aplicativos contêm várias funções de segurança. A apresentação descreve o nível de segurança alcançado da função de segurança referida no título. O nível de segurança alcançado das funções de segurança adicionais é explicado textualmente.

---

**Indicação**

O nível de segurança alcançado depende da respectiva implementação dos exemplos de aplicativos. Especialmente os pressupostos utilizados, p. ex., relativamente à frequência de manobra ou à exclusão de falhas, devem ser verificados ou mantidos.

---

Para facilitar a reprodução do aplicativo, são referidos os componentes relativos à segurança utilizados.

A funcionalidade foi testada com os componentes de hardware indicados. Também podem ser utilizados produtos semelhantes, que não constem desta lista. Tenha em atenção que nestes casos poderá ser necessário efetuar alterações na fiação dos componentes de hardware (p. ex. outra ocupação das conexões).

No fim de cada exemplo encontra-se um link de internet, onde estão guardadas informações mais detalhadas sobre o respectivo exemplo de aplicativo. Estas abrangem p. ex.

- esquemas de fiação,
- os arquivos do projeto na utilização do sistema modular de segurança
- dados CAx dos componentes de hardware utilizados

É possível consultar uma avaliação detalhada de segurança com todos os valores característicos no arquivo do projeto SET armazenado ou no relatório SET. Para a utilização do arquivo é necessária se registrar (http://www.siemens.com/safety-evaluation-tool).

Com o link de download de CAx pode descarregar (http://www.siemens.com/cax) confortavelmente toda a documentação relativa aos componentes de hardware utilizados, com apenas alguns cliques. Para o efeito, é necessário abrir uma conta no portal de serviço & assistência da Siemens ou em Siemens Industry Mall.

A parametrização dos dispositivos de comutação de segurança é feita através do interruptor DIP. A respectiva definição deve ser consultada nos esquemas elétricos armazenados.

---

**Indicação**

Os detalhes sobre prescrições e normas, bem como a especificação e o design de peças relevantes à segurança dos comandos, encontram-se no fim deste manual.

---

# 3.2 Paralisar em caso de emergência

## 3.2.1 Introdução

O aparelho de comando de parada de emergência é um componente amplamente utilizado para proteger pessoas, instalações e o ambiente de perigos e iniciar uma paralisação em caso de emergência. Neste capítulo serão descritos aplicativos com funções de segurança desta área de aplicação.

### Aplicação típica

O aparelho de comando de parada de emergência com seu contato de abertura positiva é monitorado aqui por uma unidade de avaliação. Se a paragem de emergência for acionada, a unidade de avaliação desliga os sistemas de atuadores a jusante através de saídas seguras, de acordo com a categoria de parada 0 segundo EN 60204-1. Antes da reativação ou da confirmação do desligamento de parada de emergência através do botão de arranque, é verificado se os contatos do aparelho de comando de parada de emergência estão fechados e se os sistemas de atuadores se desligaram.

---

**Indicação**

- Os cabos dos sensores devem ser instalados protegidos; como sensores deve utilizar-se exclusivamente sensores de segurança com contatos de abertura positiva.
- Os equipamentos, os aspetos funcionais e os princípios de concepção relativos à parada de emergência encontram-se em EN ISO 13850. A norma EN 60204-1 deve ser observada adicionalmente.
- O "desligar em caso de emergência" não representa um meio para a redução de riscos.
- O "desligar em caso de emergência" é uma "função de segurança complementar" (quando o "desligar em caso de emergência" é acionado, é necessário desligar o motor).

---

## Ligação inadvertida

Frequentemente existe a necessidade de proteger um aparelho de comando de parada de emergência de uma ligação inadvertida de forma a aumentar a disponibilidade do sistema. O primeiro passo é o posicionamento correto do aparelho de comando de parada de emergência na máquina. O aparelho de comando de parada de emergência tem de estar facilmente acessível, tem de ser livremente alcançável e tem de poder ser acionado sem qualquer perigo. Adicionalmente existe a possibilidade de utilizar um colar de proteção como proteção contra ligação inadvertida. Também neste caso é necessário assegurar que a acessibilidade não apresenta qualquer restrição.

---

**Indicação**

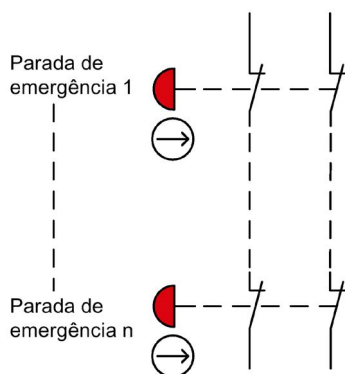
Os aparelhos de comando de parada de emergência SIEMENS SIRIUS com colar de proteção cumprem os requisitos da EN ISO 13850 "Segurança de máquinas - Desligar em caso de emergência - Princípios de concepção".

Até ao momento não existem requisitos especiais em relação aos colares de proteção, pois estes não são referidos de forma explícita em qualquer norma relativamente à segurança funcional. Frequentemente é deixado ao critério do perito especial se os aceita para uma determinada máquina.

---

## Condições para a ligação em série

Os aparelhos de comando de parada de emergência podem ser ligados em série até PL e (segundo ISO 13849-1) ou SIL 3 (segundo IEC 62061), se for possível excluir a falha e a pressão em simultâneo dos aparelhos de comando de parada de emergência.

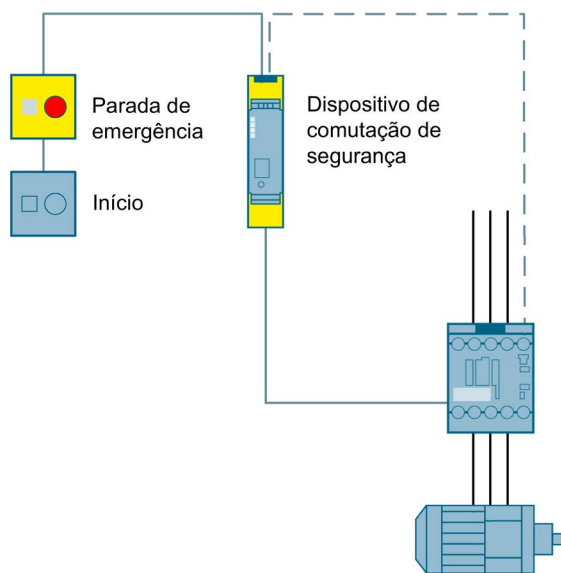
Se existirem vários aparelhos de comando de parada de emergência ligados eletricamente em série, cada desativação de segurança através de um aparelho de comando de parada de emergência representa uma função de segurança complementar individual. Se forem utilizados aparelhos de comando de parada de emergência do mesmo tipo, é suficiente considerar uma função de segurança complementar como representativa de todas as outras funções de segurança complementares, a título exemplificativo.

## Ver também

Explicação sobre a ligação em série de aparelhos de comando de parada de emergência (http://support.automation.siemens.com/WW/view/pt/35444028)

### 3.2.2 Desligamento de parada de emergência até SIL 1 ou PL c com um dispositivo de comutação de segurança

#### Aplicação

Desligamento de parada de emergência de um canal de um motor através de um dispositivo de comutação de segurança 3SK1 e contator de potência.

#### Estrutura

Esquema 3-2 Desligamento de parada de emergência até SIL 1 ou PL c com um dispositivo de comutação de segurança

## Modo de funcionamento

O dispositivo de comutação de segurança monitora o aparelho de comando de parada de emergência. Quando o aparelho de comando de parada de emergência é ligado, o dispositivo de comutação de segurança abre os circuitos de liberação e desliga de modo seguro o contator de potência. É possível ligar novamente através do botão de arranque, se o aparelho de comando de parada de emergência estiver desbloqueado e o circuito de retorno fechado.

## Componentes relativos à segurança

| Aparelho de comando de parada de emergência | Dispositivo de comutação de segurança | Contator |
|---|---|---|
| | | |
| 3SB3 (http://www.siemens.com/sirius-commanding) | 3SK1 (http://www.siemens.com/safety-relays) | 3RT20 (http://www.siemens.com/sirius-switching) |

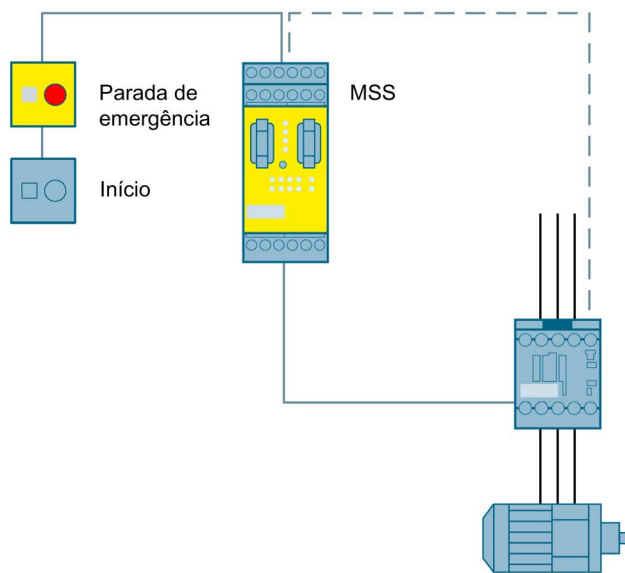
## Ver também

Esquema elétrico e avaliação SET
(http://support.automation.siemens.com/WW/view/pt/73134129)

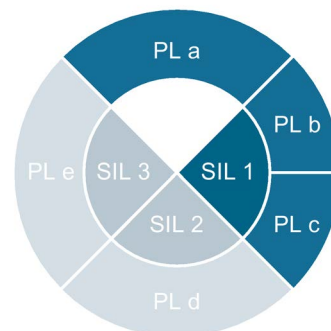
### 3.2.3 Desligamento de parada de emergência até SIL 1 ou PL c com um sistema modular de segurança

#### Aplicação

Desligamento de parada de emergência de um canal de um motor através de um sistema modular de segurança parametrizável 3RK3 e contator de potência.

#### Estrutura

Esquema 3-3 Desligamento de parada de emergência até SIL 1 ou PL c com um sistema modular de segurança

## Modo de funcionamento

O sistema modular de segurança monitora o aparelho de comando de parada de emergência. Quando o aparelho de comando de parada de emergência é ligado, o sistema modular de segurança abre os circuitos de liberação e desliga de modo seguro o contator de potência. É possível ligar novamente através do botão de arranque, se o aparelho de comando de parada de emergência estiver desbloqueado e o circuito de retorno fechado.

## Componente relativo à segurança

| Aparelho de comando de parada de emergência | Sistema modular de segurança | Contator |
| --- | --- | --- |
| | | |
| 3SB3 (http://www.siemens.com/sirius-commanding) | 3RK3 (http://www.siemens.com/sirius-mss) | 3RT20 (http://www.siemens.com/sirius-switching) |

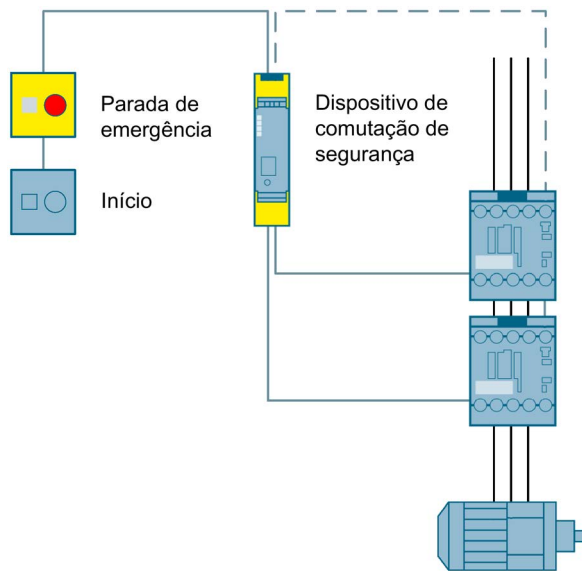
## Ver também

Esquema elétrico, projeto do sistema modular de segurança e avaliação SET (http://support.automation.siemens.com/WW/view/pt/69064058)

### 3.2.4 Desligamento de parada de emergência até SIL 3 ou PL e com um dispositivo de comutação de segurança

#### Aplicação

Desligamento de parada de emergência de dois canais de um motor através de um dispositivo de comutação de segurança 3SK1 e contatores de potência.

#### Estrutura

Esquema 3-4 Desligamento de parada de emergência até SIL 3 ou PL e com um dispositivo de comutação de segurança

## Modo de funcionamento

O dispositivo de comutação de segurança monitora o aparelho de comando de parada de emergência em dois canais. Quando o aparelho de comando de parada de emergência é ligado, o dispositivo de comutação de segurança abre os circuitos de liberação e desliga de modo seguro os contatores de potência. É possível ligar novamente através do botão de arranque, se o aparelho de comando de parada de emergência estiver desbloqueado e o circuito de retorno fechado.

## Componentes relativos à segurança

| Aparelho de comando de parada de emergência | Dispositivo de comutação de segurança | Contator |
|---|---|---|
| | | |
| 3SB3 (2 canais) (http://www.siemens.com/sirius-commanding) | 3SK1 (http://www.siemens.com/safety-relays) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

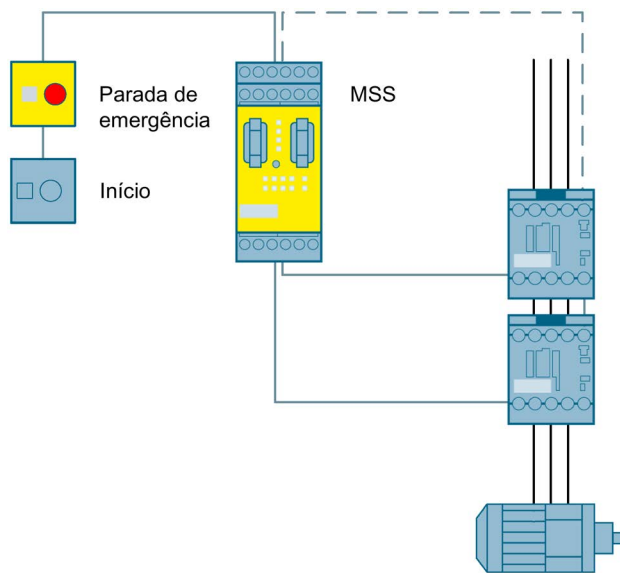
## Ver também

Esquema elétrico e avaliação SET (http://support.automation.siemens.com/WW/view/pt/73136378)

### 3.2.5 Desligamento de parada de emergência até SIL 3 ou PL e com um sistema modular de segurança

#### Aplicação

Desligamento de parada de emergência de dois canais de um motor através de um sistema modular de segurança parametrizável 3RK3 e contatores de potência.

#### Estrutura

Esquema 3-5 Desligamento de parada de emergência até SIL 3 ou PL e com um sistema modular de segurança

## Modo de funcionamento

O sistema modular de segurança monitora o aparelho de comando de parada de emergência em dois canais. Quando o aparelho de comando de parada de emergência é ligado, o sistema modular de segurança abre os circuitos de liberação e desliga de modo seguro os contatores de potência. É possível ligar novamente através do botão de arranque, se o aparelho de comando de parada de emergência estiver desbloqueado e o circuito de retorno fechado.

## Componentes relativos à segurança

| Aparelho de comando de parada de emergência | Sistema modular de segurança | Contator |
|---|---|---|
| | | |
| 3SB3 (2 canais)<br>(http://www.siemens.com/sirius-commanding) | 3RK3<br>(http://www.siemens.com/sirius-mss) | 2x 3RT20<br>(http://www.siemens.com/sirius-switching) |

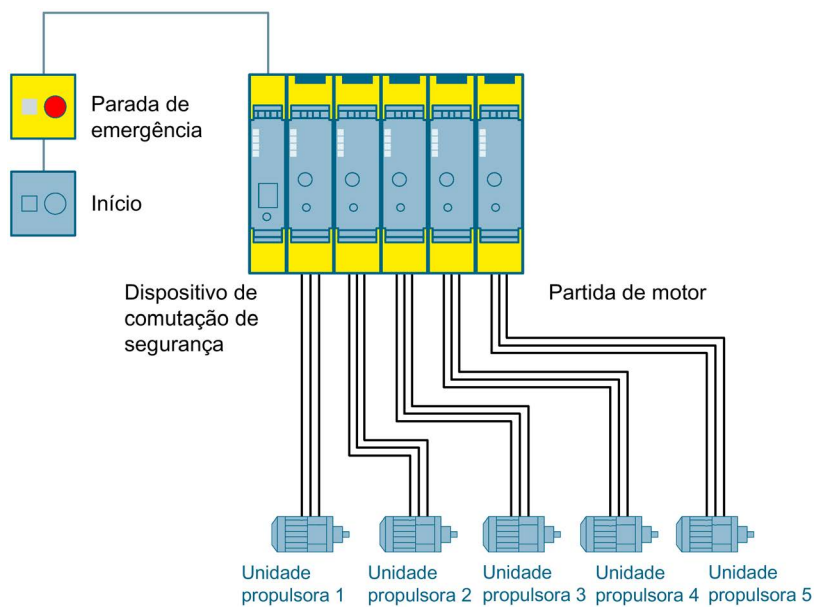
## Ver também

Esquema elétrico, projeto do sistema modular de segurança e avaliação SET (http://support.automation.siemens.com/WW/view/pt/69064698)

### 3.2.6 Desligamento de parada de emergência até SIL 3 ou PL e com partidas do motor failsafe e um dispositivo de comutação de segurança

#### Aplicação

Para que uma máquina possa ser desligada em segurança em caso de emergência, é instalado um aparelho de comando de parada de emergência que é monitorado por um dispositivo de comutação de segurança. O desligamento seguro ocorre através de uma partida do motor failsafe.

#### Estrutura

Esquema 3-6 Desligamento de parada de emergência até SIL 3 ou PL e com partidas do motor failsafe e um dispositivo de comutação de segurança

## Modo de funcionamento

O dispositivo de comutação de segurança monitora o aparelho de comando de parada de emergência. Quando o aparelho de comando de parada de emergência é ligado, o dispositivo de comutação de segurança desliga a partida do motor failsafe através do conector de dispositivos. Por conseguinte, as partidas do motor desligam a carga de forma segura. É possível ligar novamente através do botão de arranque, se o aparelho de comando de parada de emergência estiver desbloqueado.

---

**Indicação**

Neste exemplo presume-se que o perigo só advém de uma unidade propulsora, porém, numa parada de emergência terá de ser desligado um grupo de unidades propulsoras. Por este motivo, na avaliação de segurança é considerada apenas uma única partida do motor e utilizada como exemplo.

Se existir perigo devido ao movimento de várias unidades propulsoras, é necessário considerar todas as partidas do motor envolvidas no perigo, na avaliação de segurança.

---

## Componentes relativos à segurança

| Aparelho de comando de parada de emergência | Dispositivo de comutação de segurança | Arrancador motor Failsafe |
|---|---|---|
| | | |
| 3SB3 (http://www.siemens.com/sirius-commanding) | 3SK1 (http://www.siemens.com/safety-relays) | 3RM1 (http://www.siemens.com/motorstarter/3rm1) |

## Ver também

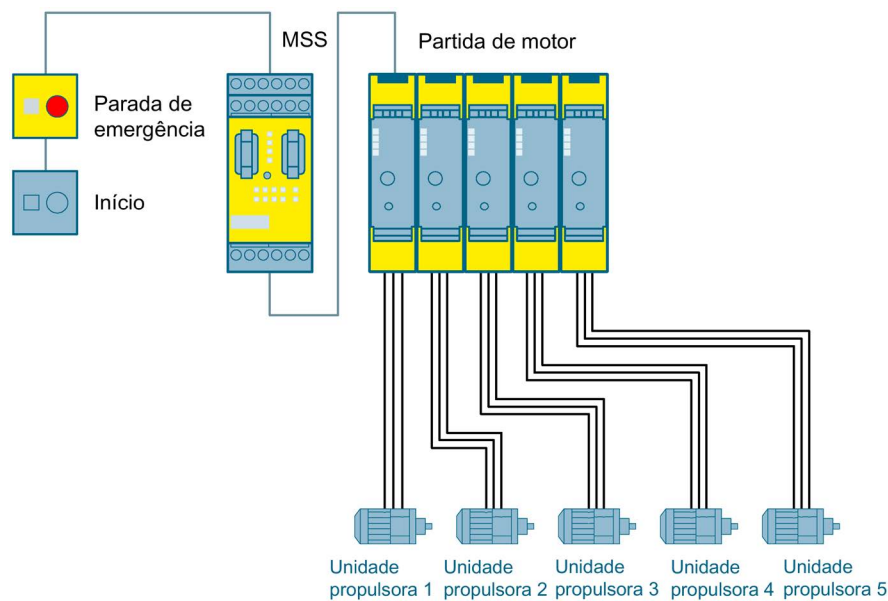
Esquema elétrico e avaliação SET (http://support.automation.siemens.com/WW/view/pt/88411471)

FAQs detalhadas sobre o tema: Desligamento seguro com as partidas do motor 3RM1 (http://support.automation.siemens.com/WW/view/pt/67478946)

### 3.2.7 Desligamento de parada de emergência até SIL 3 ou PL e com partidas do motor failsafe e um sistema modular de segurança

#### Aplicação

Para que uma máquina possa ser desligada em segurança em caso de emergência, é instalado um aparelho de comando de parada de emergência que é monitorado por um sistema modular de segurança. O desligamento seguro ocorre através de uma partida do motor failsafe.

#### Estrutura

Esquema 3-7 Desligamento de parada de emergência até SIL 3 ou PL e com partidas do motor failsafe e um sistema modular de segurança

## Modo de funcionamento

O sistema modular de segurança monitora o aparelho de comando de parada de emergência. Quando o aparelho de comando de parada de emergência é ligado, o sistema modular de segurança desliga a partida do motor failsafe. Por conseguinte, as partidas do motor desligam a carga de forma segura. É possível ligar novamente através do botão de arranque, se o aparelho de comando de parada de emergência estiver desbloqueado.

### Indicação

Neste exemplo presume-se que o perigo só advém de uma unidade propulsora, porém, numa parada de emergência terá de ser desligado um grupo de unidades propulsoras. Por este motivo, na avaliação de segurança é considerada apenas uma única partida do motor e utilizada como exemplo.

Se existir perigo devido ao movimento de várias unidades propulsoras, é necessário considerar todas as partidas do motor envolvidas no perigo, na avaliação de segurança.

### Indicação

Este exemplo aplica-se para a montagem dentro de um armário de distribuição. Se a lógica e os sistemas de atuadores não se encontrarem no mesmo armário de distribuição, devem ser tomadas outras medidas, como por exemplo uma instalação de cabos à prova de circuito transversal do sinal de desativação.

## Componentes relativos à segurança

| Aparelho de comando de parada de emergência | Sistema modular de segurança | Arrancador motor Failsafe |
| --- | --- | --- |
| | | |
| 3SB3 (http://www.siemens.com/sirius-commanding) | 3RK3 (http://www.siemens.com/sirius-mss) | 3RM1 (http://www.siemens.com/motorstarter/3rm1) |

### Ver também

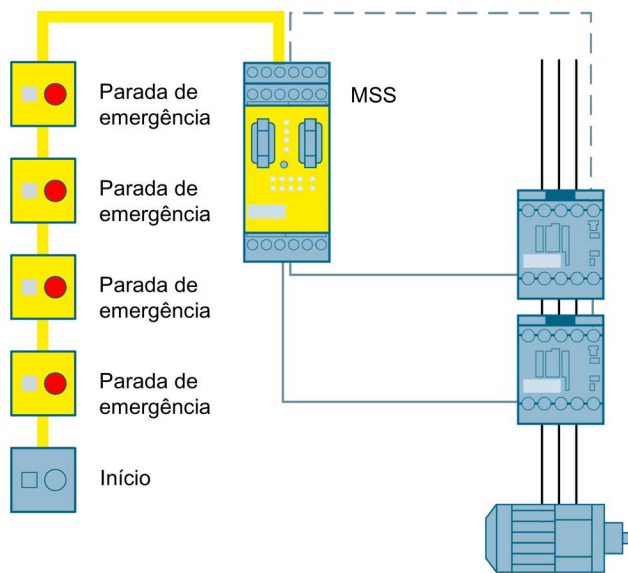
Esquema elétrico, projeto do sistema modular de segurança e avaliação SET (http://support.automation.siemens.com/WW/view/pt/88822643)

FAQs detalhadas sobre o tema: Desligamento seguro com as partidas do motor 3RM1 (http://support.automation.siemens.com/WW/view/pt/67478946)

### 3.2.8 Desligamento de parada de emergência através de AS-i até SIL 3 ou PL e com um sistema modular de segurança

#### Aplicação

Monitoramento de vários aparelhos de comando de parada de emergência através de AS-i com um sistema modular de segurança 3RK3.

#### Estrutura

Esquema 3-8 Desligamento de parada de emergência através de AS-i até SIL 3 ou PL e com um sistema modular de segurança

## Modo de funcionamento

O sistema modular de segurança monitora cada aparelho de comando de parada de emergência de dois canais ligado a AS-i. Quando um dos aparelhos de comando de parada de emergência é ligado, o sistema modular de segurança abre os circuitos de liberação e desliga de modo seguro os contatores de potência. É possível ligar novamente através do botão de arranque, se o aparelho de comando de parada de emergência estiver desbloqueado e o circuito de retorno fechado.

## Componentes relativos à segurança

| Aparelho de comando de parada de emergência | Sistema modular de segurança | Contator |
|---|---|---|
| | | |
| 3SB3 (2 canais) (http://www.siemens.com/sirius-commanding) | 3RK3 (http://www.siemens.com/sirius-mss) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

### Indicação

Adicionalmente aos componentes relativos à segurança, é necessário um AS-i-Master e um elemento de rede AS-i para operar uma rede AS-i.

## Ver também

Projeto do sistema modular de segurança e avaliação SET (http://support.automation.siemens.com/WW/view/pt/73133559)

# 3.3 Monitoramento da porta de proteção

## 3.3.1 Introdução

Este capítulo descreve aplicativos com instalações de proteção seccionadoras na forma de uma porta de proteção. A solução mais utilizada na área de instalações e máquinas é a proteção de áreas de perigo com instalações de proteção seccionadoras mecânicas ou portinholas de acesso. Neste caso, é necessário monitorar o acesso não autorizado às áreas da instalação, bem como evitar uma função da máquina que acarrete perigo quando a instalação de proteção não está fechada. O monitoramento da instalação de proteção tanto pode ser feito com interruptores de posição ou de segurança mecânicos, como com interruptores de segurança numa base magnética ou RFID.

Frequentemente também é realizada uma retenção da porta de proteção paralelamente ao monitoramento da mesma. Os dispositivos de travamento com retenção servem para proteger as áreas de perigo de acesso inadvertido. Isso geralmente tem dois motivos:

1. Para proteger as pessoas de movimentos subsequentes e perigosos da máquina, de elevadas temperaturas, etc.. Sobre este assunto, a ISO 14119 ou a EN 1088 fornece os princípios orientadores para a disposição e seleção de dispositivos de travamento. Nesta norma é requerido que a área de perigo só fique acessível após a parada dos movimentos perigosos da máquina.
2. Uma retenção pode fazer sentido por motivos da segurança do processo. Este caso verifica-se quando o perigo é excluído após a abertura da instalação de proteção mas ainda existe o risco de a máquina ou a peça ficar danificada. Aqui a máquina é primeiro deslocada para uma posição de parada adequada, antes de o acesso ser aprovado.

### Interruptor de posição

Os interruptores de posição são geralmente utilizados como interruptores forçados em portas de proteção. Se a porta de proteção for aberta, o interruptor de posição é acionado e o interruptor é aberto de forma fiável (ver Conceitos básicos (Página 11): "Abertura positiva").

### Interruptor de segurança mecânico (com acionador separado)

Contrariamente aos interruptores de posição, os interruptores de segurança não podem ser facilmente enganados. O interruptor de segurança só pode ser ligado com o respectivo acionador codificado.

### Interruptor de segurança mecânico (interruptor de charneira)

Os interruptores de charneira são utilizados nos locais onde, por motivos de segurança, é necessário monitorar a posição de instalações de proteção basculáveis, tais como portas e portinholas.

### Interruptor de segurança mecânico (com retenção)

Os interruptores de segurança com retenção são equipamentos de segurança especiais, os quais impedem a abertura inadvertida ou propositada de portas de proteção, grelhas de proteção ou outras coberturas enquanto persistir uma situação perigosa. (p. ex. marcha por inércia da máquina). Neste tipo de interruptores, também é efetuada uma detecção da posição com a ajuda de um acionador separado, independentemente da retenção.

### Interruptor de segurança sem contato (comutador magnético)

Os comutadores magnéticos são constituídos por um ímã de comutação codificado e um elemento de comutação. Foram concebidos para serem montados em instalações de proteção móveis e, devido à sua forma de construção fechada, são especialmente adequados para áreas afetadas por uma poluição elevada e por produtos de limpeza e de desinfecção.

### Interruptor de segurança (RFID)

Os interruptores de segurança RFID são constituídos por um interruptor RFID codificado e por um acionador RFID de estrutura idêntica e podem ser amplamente utilizados, especialmente em áreas com condições ambientais extremas. Os interruptores também são ideais para máquinas de processamento de metal, graças ao princípio de ação eletrônico. Os interruptores possuem uma distância de chaveamento maior do que os dispositivos de comutação mecânicos e oferecem uma tolerância de montagem melhor bem como possibilidades de diagnóstico abrangentes. Para além disso, oferecem também uma proteção máxima contra manipulação através da codificação individual do interruptor e do acionador.

## Aplicação típica

A porta de proteção é monitorada por interruptores de posição SIRIUS com contatos de abertura positiva através de uma unidade de avaliação. Se esta porta de proteção for aberta, a unidade de avaliação desliga os atuadores a jusante através de saídas seguras, de acordo com a categoria de parada 0 segundo EN 60204-1. Se a porta de proteção for fechada, ocorre a reativação no caso de arranque automático, após a verificação do interruptor de posição e dos atuadores a jusante. No caso de arranque manual, isso só ocorre após a ligação do botão de arranque.

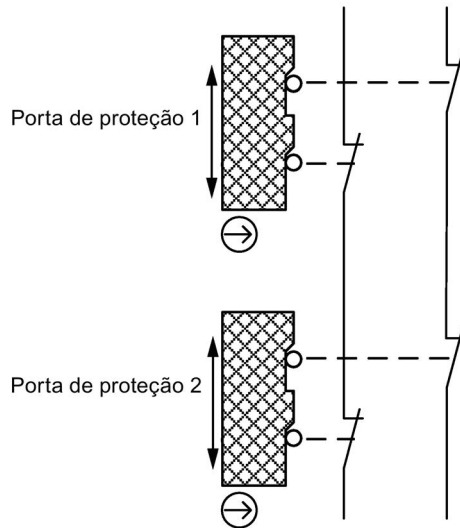
---

**Indicação**

- Os interruptores de posição devem ser dispostos de modo que não sejam danificados durante o acionamento e a ultrapassagem. Portanto, eles não podem ser utilizados como encostos mecânicos.
- Os cabos dos sensores devem ser instalados protegidos; como sensores deve utilizar-se exclusivamente sensores de segurança com contatos de abertura positiva.
- A retenção representa uma função de segurança individual e separada, paralelamente à função de segurança do monitoramento da porta de proteção através de interruptores de posição. O acionamento pode ter uma integridade de segurança solicitada um nível mais baixo do que aquilo que a avaliação de risco calculou para o monitoramento da porta de proteção. (Razão: A probabilidade de as duas funções de segurança falharem ao mesmo tempo pode ser quase excluída. Exemplo:
  a monitorização da porta de proteção é solicitada em PL d ou SIL 2, o acionamento do dispositivo de retenção pode ser realizado em PL c ou SIL 1

---

## Condições para a ligação em série

Os interruptores de posição só podem ser ligados em série até PL d (segundo ISO 13849-1) ou SIL 2 (segundo IEC 62061), se for possível excluir que não são abertas frequentemente várias portas de proteção em simultâneo (caso contrário, não é possível ocorrer uma detecção de erros). Não é possível realizar uma ligação em série em PL e (segundo ISO 13849-1) ou SIL 3 (segundo IEC62061).

## Combinação possível para a detecção da posição e nível de segurança alcançável

Os exemplos de aplicativos neste capítulo só conseguem cobrir uma parte das combinações possíveis de aparelhos de registro para a detecção da posição. A tabelas seguintes indicam de uma forma simples o nível de segurança máximo que pode ser alcançado com um determinado tipo de detecção da posição.

Tabelas 3- 1 **Monitoramento seguro da posição com dispositivos de comutação mecânicos**

| **Unidades de avaliação** | | | Interruptor de posição | Interruptor de segurança Interruptor de charneira | Interruptor de segurança com acionador separado | Interruptor de segurança com função de retenção opcional |
|---|---|---|---|---|---|---|
| **Nível de segurança alcançável com UM interruptor de posição** | **Monitoramento de um contato de interrupção** | | SIL 1 / PL c | SIL 1 / PL c | SIL 1 / PL c | SIL 1 / PL c |
| | **Monitoramento de 2 contatos de interrupção ou 1 contato NF + 1 contato NA** | | SIL 1 / PL c | SIL 2 / PL d | SIL 2 / PL d | SIL 2 / PL d |
| **Nível de segurança alcançável com DOIS interruptores de posição** | Interruptor de posição | | SIL 3 / PL e | SIL 3 / PL e | SIL 3 / PL e | SIL 3 / PL e |
| | Interruptor de segurança Interruptor de charneira | | SIL 3 / PL e | SIL 3 / PL e | SIL 3 / PL e | SIL 3 / PL e |
| | Interruptor de segurança com acionador separado | | SIL 3 / PL e | SIL 3 / PL e | SIL 3 / PL e | SIL 3 / PL e |
| | Interruptor de segurança com função de retenção opcional | | SIL 3 / PL e | SIL 3 / PL e | SIL 3 / PL e | SIL 3 / PL e |

### Exemplo 1:

Mediante a combinação de dois interruptores de segurança mecânicos (com acionador separado) é possível alcançar um nível de segurança de até PL e ou SIL 3.

### Exemplo 2:

Na utilização de um interruptor de segurança mecânico (interruptor de charneira) é possível alcançar um nível de segurança de até PL d ou SIL 2.

Tabelas 3- 2 Retenção segura da porta de proteção

| **Unidades de avaliação seguras** | **Interruptor de segurança** | |
|---|---|---|
| | Interruptor de segurança com retenção | Interruptor de segurança com retenção |
| Sistema modular de segurança 3RK3 | SIL 2 / PL d | SIL 3 / PL e |
| Dispositivo de comutação de segurança 3TK2845 | SIL 2 / PL d | SIL 3 / PL e |

---

**Indicação**

Geralmente, para a utilização deste interruptor de posição, é necessário assegurar um acionamento forçado através da construção da instalação de proteção. Apenas sob esta condição é que os valores referidos na tabela são admissíveis.

---

**Indicação**

Considerando determinadas exclusões de falhas (p. ex. quebra do acionador), é possível a utilização de apenas um interruptor de charneira ou de um interruptor com acionador separado até SIL 2 ou PL d, tal como descrito na tabela. O fabricante dos componentes não pode efetuar uma avaliação definitiva das medidas adotadas, devido ao fato de o fabricante da máquina ter de comprovar a exclusão de falhas.

Para mais informações consulte o documento no seguinte link: http://support.automation.siemens.com/WW/view/de/35443942.

---

### Indicação

No caso de uma montagem de dois canais com sensores eletromecânicos, só é possível alcançar SIL 3 ou PL e se os sensores forem alimentados através da unidade de avaliação. Só assim é possível um diagnóstico suficiente.

Tabelas 3- 3 **Monitoramento seguro da posição com interruptores de segurança**

| **Unidades de avaliação seguras** | Aparelhos de registro<br>Interruptor de segurança | |
|---|---|---|
| | Comutador magnético<br>3SE66 / 3SE67 | Interruptor de segurança<br>RFID<br>3SE63 |
| Dispositivo de comutação de segurança 3SK1 | SIL 3 / PL e | SIL 3 / PL e |
| Sistema modular de segurança 3RK3 | SIL 3 / PL e | SIL 3 / PL e |

### Indicação

Os níveis de segurança alcançáveis dependem também do tipo de unidade de avaliação de segurança utilizada (especialmente a respectiva capacidade de diagnóstico).

### Ver também

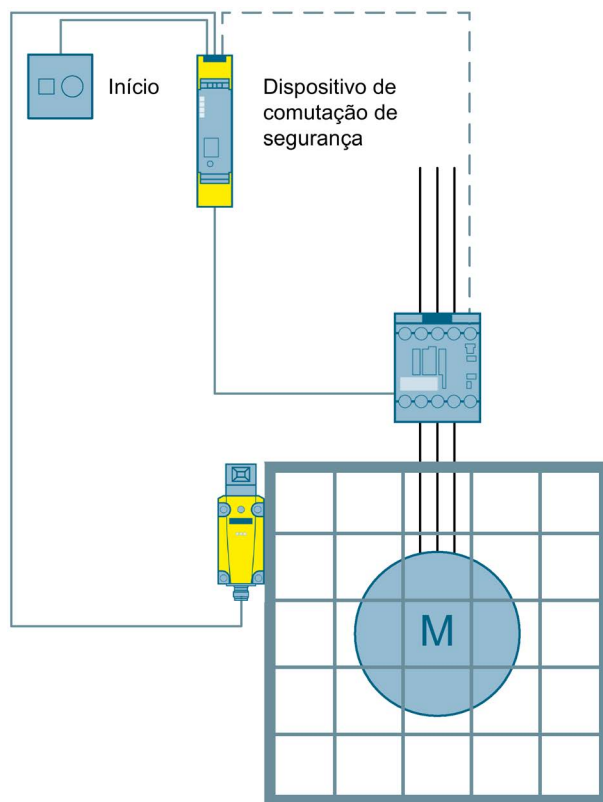
Monitoramento e retenção de uma porta de proteção com sistema modular de segurança (MSS) (http://support.automation.siemens.com/WW/view/pt/62837891)

Nível de segurança alcançável mediante a utilização de apenas um interruptor de posição SIRIUS com ou sem retenção (http://support.automation.siemens.com/WW/view/pt/35443942)

## 3.3.2 Monitoramento da porta de proteção até SIL 1 ou PL c com um dispositivo de comutação de segurança

### Aplicação

Para a delimitação de áreas de perigo são utilizadas frequentemente portas de proteção. Estas são monitoradas quanto à sua posição e, se necessário, é desligada a área da qual advém o perigo.

### Estrutura

Esquema 3-9 Monitoramento da porta de proteção até SIL 1 ou PL c com um dispositivo de comutação de segurança

## Modo de funcionamento

A posição de uma porta de proteção é monitorada através do contato do interruptor de segurança. Com a abertura da porta monitorada, o dispositivo de comutação de segurança é acionado e abre os circuitos de liberação provocando o desligamento seguro do contator de potência. É possível ligar novamente através do botão de arranque, se a porta e o circuito de retorno estiverem fechados.

## Componentes relativos à segurança

| Interruptor de segurança | Dispositivo de comutação de segurança | Contator |
|---|---|---|
| | | |
| 3SE5 (http://www.siemens.com/sirius-detecting) | 3SK1 (http://www.siemens.com/safety-relays) | 3RT20 (http://www.siemens.com/sirius-switching) |

## Ver também

Esquema elétrico e avaliação SET (http://support.automation.siemens.com/WW/view/pt/73135973)

### 3.3.3 Monitoramento da porta de proteção até SIL 1 ou PL c com um sistema modular de segurança

#### Aplicação

Para a delimitação de áreas de perigo são utilizadas frequentemente portas de proteção. Estas são monitoradas quanto à sua posição e, se necessário, é desligada a área da qual advém o perigo.

#### Estrutura

Esquema 3-10 Monitoramento da porta de proteção até SIL 1 ou PL c com um sistema modular de segurança

## Modo de funcionamento

A posição de uma porta de proteção é monitorada através do contato do interruptor de segurança. Com a abertura da porta monitorada, o sistema modular de segurança é acionado e abre os circuitos de liberação provocando o desligamento seguro do contator de potência. É possível ligar novamente através do botão de arranque, se a porta e o circuito de retorno estiverem fechados.

## Componentes relativos à segurança

| Interruptor de segurança | Sistema modular de segurança | Contator |
|---|---|---|
| | | |
| 3SE5 (http://www.siemens.com/sirius-detecting) | 3RK3 (http://www.siemens.com/sirius-mss) | 3RT20 (http://www.siemens.com/sirius-switching) |

## Ver também

Esquema elétrico, projeto do sistema modular de segurança e avaliação SET (http://support.automation.siemens.com/WW/view/pt/69064060)

### 3.3.4 Monitoramento da porta de proteção até SIL 3 ou PL e com um dispositivo de comutação de segurança

#### Aplicação

Para a delimitação de áreas de perigo são utilizadas frequentemente portas de proteção. Estas são monitoradas quanto à sua posição e, se necessário, é desligada a área da qual advém o perigo.

#### Estrutura

Esquema 3-11 Monitoramento da porta de proteção até SIL 3 ou PL e com um dispositivo de comutação de segurança

## Modo de funcionamento

A posição de uma porta de proteção é monitorada através de dois interruptores de segurança. Com a abertura da porta monitorada, o dispositivo de comutação de segurança é acionado e abre os circuitos de liberação provocando o desligamento seguro dos contatores de potência. É possível ligar novamente através do botão de arranque, se a porta e o circuito de retorno estiverem fechados.

## Componentes relativos à segurança

| Interruptor de posição | | Dispositivo de comutação de segurança | Contator |
|---|---|---|---|
| | | | |
| 2x 3SE5 (http://www.siemens.com/sirius-detecting) | | 3SK1 (http://www.siemens.com/safety-relays) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

## Ver também

Esquema elétrico e avaliação SET
(http://support.automation.siemens.com/WW/view/pt/73135309)

### 3.3.5 Monitoramento da porta de proteção até SIL 3 ou PL e com um sistema modular de segurança

#### Aplicação

Para a delimitação de áreas de perigo são utilizadas frequentemente portas de proteção. Estas são monitoradas quanto à sua posição e, se necessário, é desligada a área da qual advém o perigo.

#### Estrutura

Esquema 3-12 Monitoramento da porta de proteção até SIL 3 ou PL e com um sistema modular de segurança

## Modo de funcionamento

A posição de uma porta de proteção é monitorada através de dois interruptores de segurança. Com a abertura da porta monitorada, o sistema modular de segurança é acionado e abre os circuitos de liberação provocando o desligamento seguro dos contatores de potência. É possível ligar novamente através do botão de arranque, se a porta e o circuito de retorno estiverem fechados.

## Componentes relativos à segurança

| Interruptor de posição | Sistema modular de segurança | Contator |
|---|---|---|
| 2x 3SE5 (http://www.siemens.com/sirius-detecting) | 3RK3 (http://www.siemens.com/sirius-mss) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

## Ver também

Esquema elétrico, projeto do sistema modular de segurança e avaliação SET (http://support.automation.siemens.com/WW/view/pt/69064861)

### 3.3.6 Monitoramento da porta de proteção até SIL 3 ou PL e com uma partida do motor failsafe e um dispositivo de comutação de segurança

#### Aplicação

Para a delimitação de áreas de perigo são utilizadas frequentemente portas de proteção. Estas são monitoradas quanto à sua posição e, se necessário, é desligada a área da qual advém o perigo.

#### Estrutura

Esquema 3-13 Monitoramento da porta de proteção até SIL 3 ou PL e com uma partida do motor failsafe e um dispositivo de comutação de segurança

## Modo de funcionamento

A posição de uma porta de proteção é monitorada através do contato do interruptor de segurança. Com a abertura da porta monitorada, o dispositivo de comutação de segurança é acionado e desliga a partida do motor failsafe através do conector de dispositivos. Por conseguinte, a partida do motor desliga a carga de forma segura. É possível ligar novamente através do botão de arranque, se a porta estiver fechada.

## Componentes relativos à segurança

| Interruptor de segurança | Dispositivo de comutação de segurança | Arrancador motor Failsafe |
|---|---|---|
| | | |
| 2x 3SE5 (http://www.siemens.com/sirius-detecting) | 3SK1 (http://www.siemens.com/safety-relays) | 3RM1 (http://www.siemens.com/motorstarter/3rm1) |

## Ver também

Esquema elétrico e avaliação SET (http://support.automation.siemens.com/WW/view/pt/88822953)

FAQs detalhadas sobre o tema: Desligamento seguro com as partidas do motor 3RM1 (http://support.automation.siemens.com/WW/view/pt/67478946)

### 3.3.7 Monitoramento da porta de proteção até SIL 3 ou PL e com uma partida do motor failsafe e um sistema modular de segurança

#### Aplicação

Para a delimitação de áreas de perigo são utilizadas frequentemente portas de proteção. Estas são monitoradas quanto à sua posição e, se necessário, é desligada a área da qual advém o perigo.

#### Estrutura

Esquema 3-14 Monitoramento da porta de proteção até SIL 3 ou PL e com uma partida do motor failsafe e um sistema modular de segurança

## Modo de funcionamento

A posição de uma porta de proteção é monitorada através do contato do interruptor de segurança. Com a abertura da porta monitorada, o sistema modular de segurança é acionado e desliga a partida do motor de forma segura. Por conseguinte, a partida do motor desliga a carga de forma segura. É possível ligar novamente através do botão de arranque, se a porta e o circuito de retorno estiverem fechados.

### Indicação

Este exemplo aplica-se para a montagem dentro de um armário de distribuição. Se a lógica e os sistemas de atuadores não se encontrarem no mesmo armário de distribuição, devem ser tomadas outras medidas, como por exemplo uma instalação de cabos à prova de circuito transversal do sinal de desativação.

## Componentes relativos à segurança

| Interruptor de segurança | Sistema modular de segurança | Arrancador motor Failsafe |
|---|---|---|
| 2x 3SE5 (http://www.siemens.com/sirius-detecting) | 3RK3 (http://www.siemens.com/sirius-mss) | 3RM1 (http://www.siemens.com/motorstarter/3rm1) |

## Ver também

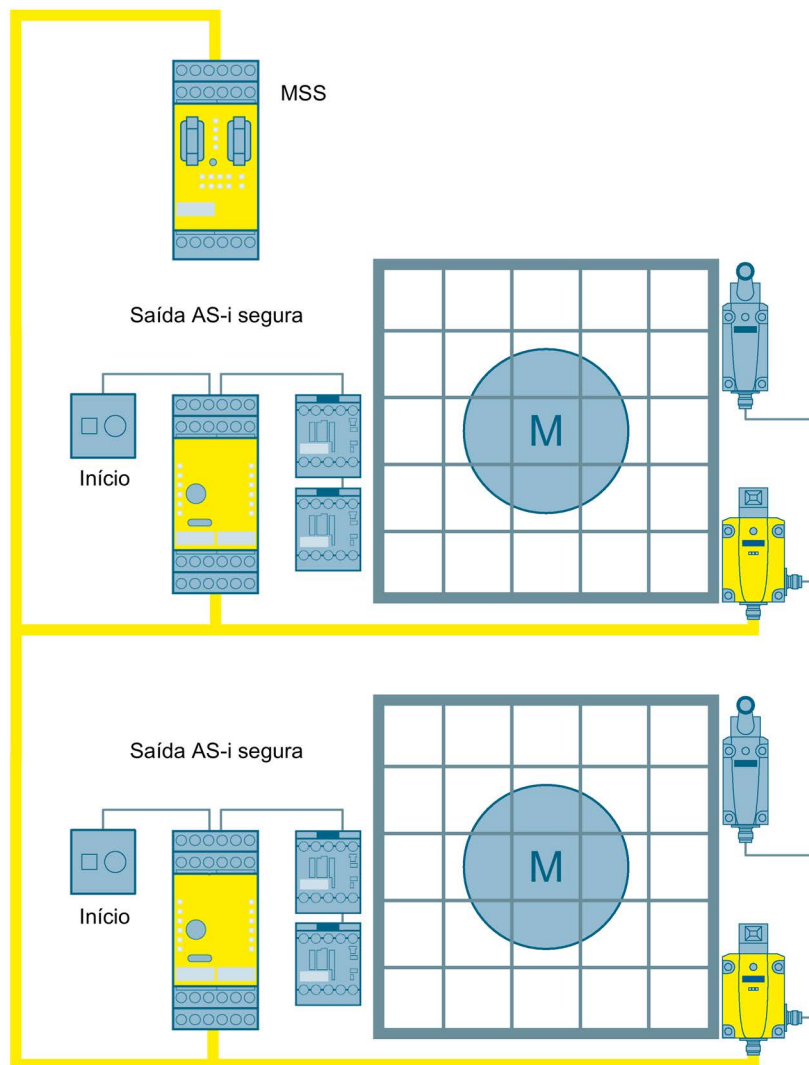
Esquema elétrico, projeto do sistema modular de segurança e avaliação SET (http://support.automation.siemens.com/WW/view/pt/88822778)

FAQs detalhadas sobre o tema: Desligamento seguro com as partidas do motor 3RM1 (http://support.automation.siemens.com/WW/view/pt/67478946)

### 3.3.8 Monitoramento da porta de proteção através de AS-i até SIL 3 ou PL e com um sistema modular de segurança

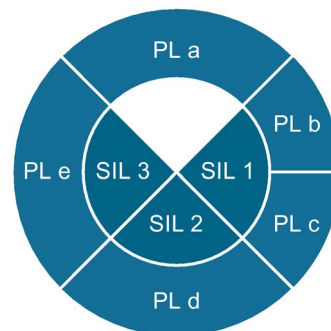
#### Aplicação

Monitoramento de várias portas de proteção e acionamento dos sistemas de atuadores através de AS-i com um sistema modular de segurança.

#### Estrutura

Esquema 3-15 Monitoramento da porta de proteção através de AS-i até SIL 3 ou PL e com um sistema modular de segurança

## Modo de funcionamento

O sistema modular de segurança monitora os interruptores de segurança ligados a AS-i e envia sinais de estado sob a forma de escravos AS-i simulados através do transmissor AS-i. Estes escravos simulados são monitorados pelas saídas AS-i seguras. Quando uma das portas de proteção é aberta, o sistema modular de segurança interrompe o respectivo sinal de estado. A saída AS-i segura abre de seguida o circuito de liberação e os contatores de potência se desligam de forma segura.

Os sinais do botão de arranque e dos contatos auxiliares do contator são enviados da saída AS-i segura através do transmissor AS-i para o sistema modular de segurança, e aí avaliados. É possível ligar novamente através do botão de arranque, se a respectiva porta de proteção e o circuito de retorno estiverem fechados.

## Componentes relativos à segurança

| Interruptor de posição | Sistema modular de segurança | Saída AS-i segura | Contator |
|---|---|---|---|
| 2x 3SE5 (http://www.siemens.com/sirius-detecting) | 3RK3 (http://www.siemens.com/sirius-mss) | 3RK1405 (www.siemens.com/as-interface) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

### Indicação

Adicionalmente aos componentes relativos à segurança, é necessário um AS-i-Master e um elemento de rede AS-i para operar uma rede AS-i.

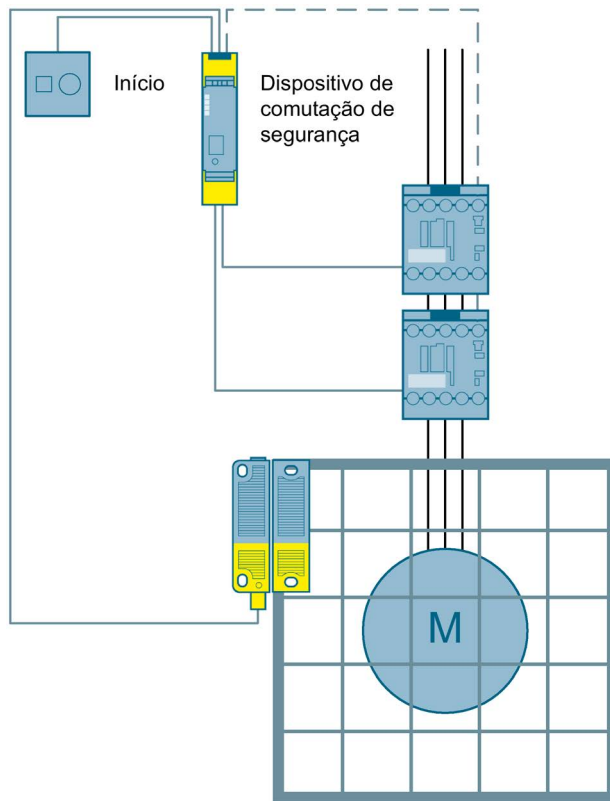
## Ver também

Esquema elétrico, projeto do sistema modular de segurança e avaliação SET (http://support.automation.siemens.com/WW/view/pt/73135311)

### 3.3.9 Monitoramento da porta de proteção através de interruptor RFID até SIL 3 ou PL e com um dispositivo de comutação de segurança

#### Aplicação

Para a delimitação de áreas de perigo são utilizadas frequentemente portas de proteção. Estas são monitoradas quanto à sua posição e, se necessário, é desligada a área da qual advém o perigo.

#### Estrutura

Esquema 3-16 Monitoramento da porta de proteção através de interruptor RFID até SIL 3 ou PL e com um dispositivo de comutação de segurança

## Modo de funcionamento

A posição de uma porta de proteção é monitorada através do interruptor de segurança. Com a abertura da porta monitorada, o dispositivo de comutação de segurança é acionado e abre os circuitos de liberação provocando o desligamento seguro dos contatores de potência. É possível ligar novamente através do botão de arranque, se a porta e o circuito de retorno estiverem fechados.

O interruptor de segurança 3SE6315 está estruturado internamente com dois canais e possui uma capacidade de diagnóstico própria. Assim, e devido à sua constituição isenta de manipulação e baseada em tecnologia RFID, não é necessário qualquer interruptor de segurança redundante para se alcançar PL e segundo ISO 13849-1 ou SIL 3 segundo IEC 62061.

## Componentes relativos à segurança

| Interruptor de segurança | Dispositivo de comutação de segurança | Contator |
|---|---|---|
| | | |
| 3SE6315 (http://www.siemens.com/sirius-detecting) | 3SK1 (http://www.siemens.com/safety-relays) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

## Ver também

Esquema elétrico e avaliação SET
(http://support.automation.siemens.com/WW/view/pt/73134150)

### 3.3.10 Monitoramento da porta de proteção através de interruptor RFID até SIL 3 ou PL e com um sistema modular de segurança

#### Aplicação

Para a delimitação de áreas de perigo são utilizadas frequentemente portas de proteção. Estas são monitoradas quanto à sua posição e, se necessário, é desligada a área da qual advém o perigo.

#### Estrutura

Esquema 3-17 Monitoramento da porta de proteção através de interruptor RFID até SIL 3 ou PL e com um sistema modular de segurança

## Modo de funcionamento

A posição de uma porta de proteção é monitorada através do interruptor de segurança. Com a abertura da porta monitorada, o sistema modular de segurança é acionado e abre os circuitos de liberação provocando o desligamento seguro dos contatores de potência. É possível ligar novamente através do botão de arranque, se a porta e o circuito de retorno estiverem fechados.

O interruptor de segurança 3SE6315 está estruturado internamente com dois canais e possui uma capacidade de diagnóstico própria. Assim, e devido à sua constituição isenta de manipulação e baseada em tecnologia RFID, não é necessário qualquer interruptor de segurança redundante para se alcançar PL e segundo ISO 13849-1 ou SIL 3 segundo IEC 62061.

## Componentes relativos à segurança

| Interruptor de segurança | Sistema modular de segurança | Contator |
|---|---|---|
| | | |
| 3SE6315 (http://www.siemens.com/sirius-detecting) | 3RK3 (http://www.siemens.com/sirius-mss) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

## Ver também

Esquema elétrico, projeto do sistema modular de segurança e avaliação SET (http://support.automation.siemens.com/WW/view/pt/69064862)

### 3.3.11 Monitoramento da porta de proteção com retenção até SIL 2 ou PL d com um dispositivo de comutação de segurança

#### Aplicação

Para a delimitação de áreas de perigo são utilizadas frequentemente portas de proteção. Estas são monitoradas quanto à sua posição e, se necessário, é desligada a área da qual advém o perigo. Se após o desligamento ainda advir algum perigo da máquina durante um determinado período de tempo, o acesso pode ser impedido durante esse período através de uma retenção.

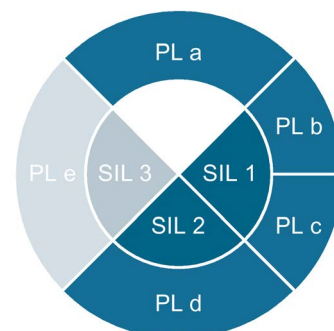
#### Estrutura

Esquema 3-18 Monitoramento da porta de proteção com retenção até SIL 2 ou PL d com um dispositivo de comutação de segurança

## Modo de funcionamento

A posição de uma porta de proteção é monitorada através de um interruptor de segurança. Adicionalmente, a porta é bloqueada através do interruptor de segurança. Se for dado o comando para o desbloqueio da porta, o dispositivo de comutação de segurança é acionado e abre os circuitos de liberação provocando o desligamento seguro dos contatores de potência. A retenção é debloqueada depois de decorrido o tempo definido. É possível ligar novamente através do botão de arranque, se a porta estiver fechada e bloqueada e o circuito de retorno fechado.

Tanto a função de segurança "Monitoramento da porta de proteção" como também a função de segurança "Retenção da porta de proteção" foram concebidas até SIL 2 ou PL d.

Considerando as exclusões de falhas, é permitida a utilização de apenas um interruptor de segurança com ou sem retenção até SIL 2 ou PL d. Para mais informações consulte o documento referido em baixo.

## Componentes relativos à segurança

| Interruptor de segurança com retenção | Dispositivo de comutação de segurança | Contator |
|---|---|---|
| | | |
| 3SE5 (http://www.siemens.com/sirius-detecting) | 3TK2845 (http://www.automation.siemens.com/mcms/industrial-controls/en/safety-systems/3tk28) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

## Ver também

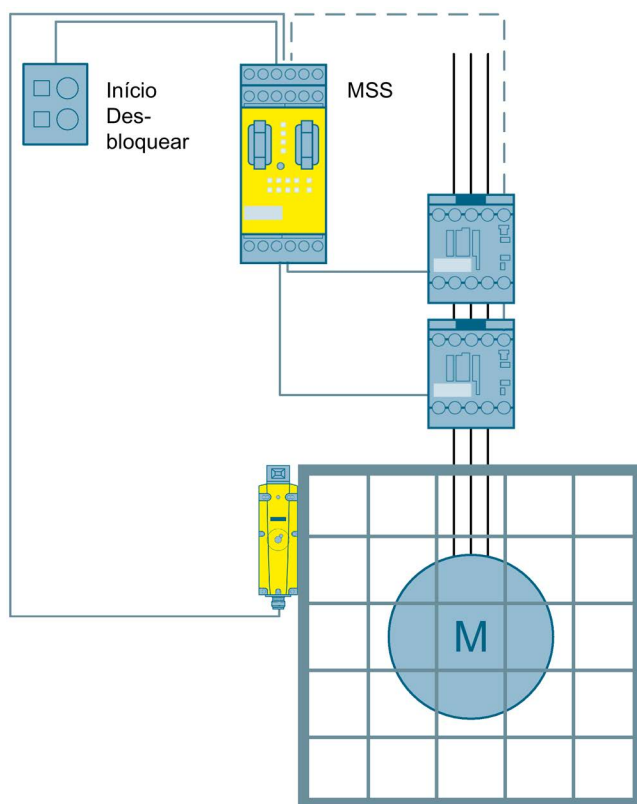
Esquema elétrico e avaliação SET (http://support.automation.siemens.com/WW/view/pt/73136328)

Documento sobre a utilização de interruptores de segurança até SIL 2 ou PL d (http://support.automation.siemens.com/WW/view/pt/35443942)

### 3.3.12 Monitoramento da porta de proteção com retenção até SIL 2 ou PL d com um sistema modular de segurança

#### Aplicação

Para a delimitação de áreas de perigo são utilizadas frequentemente portas de proteção. Estas são monitoradas quanto à sua posição e, se necessário, é desligada a área da qual advém o perigo. Se após o desligamento ainda advir algum perigo da máquina durante um determinado período de tempo, o acesso pode ser impedido durante esse período através de uma retenção.

#### Estrutura

Esquema 3-19 Monitoramento da porta de proteção com retenção até SIL 2 ou PL d com um sistema modular de segurança

## Modo de funcionamento

A posição de uma porta de proteção é monitorada através de um interruptor de segurança. Adicionalmente, a porta é bloqueada através do interruptor de segurança. Se for dado o comando para o desbloqueio da porta, o dispositivo de comutação de segurança é acionado e abre os circuitos de liberação provocando o desligamento seguro dos contatores de potência. A retenção é desbloqueada depois de decorrido o tempo definido. É possível ligar novamente através do botão de arranque, se a porta estiver fechada e bloqueada e o circuito de retorno fechado.

Tanto a função de segurança "Monitoramento da porta de proteção" como também a função de segurança "Retenção da porta de proteção" foram concebidas até SIL 2 ou PL d.

Considerando as exclusões de falhas, é permitida a utilização de apenas um interruptor de segurança com ou sem retenção até SIL 2 ou PL d. Para mais informações consulte o documento referido em baixo.

## Componentes relativos à segurança

| Interruptor de segurança com retenção | Sistema modular de segurança | Contator |
|---|---|---|
| | | |
| 3SE5 (http://www.siemens.com/sirius-detecting) | 3RK3 (http://www.siemens.com/sirius-mss) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

## Ver também

Esquema elétrico, projeto do sistema modular de segurança e avaliação SET (http://support.automation.siemens.com/WW/view/pt/73137468)

Documento sobre a utilização de interruptores de segurança até SIL 2 ou PL d (http://support.automation.siemens.com/WW/view/pt/35443942)

## 3.4 Monitoramento de áreas de perigo abertas

### 3.4.1 Introdução

Dentro de uma empresa industrial existem frequentemente áreas que não podem estar acessíveis às pessoas durante determinados períodos de tempo, devido ao elevado perigo. Assim, não é permitido, por exemplo, que se encontre qualquer parte do corpo dentro de uma prensa durante o movimento descendente. Tais monitoramentos são frequentemente realizados por cortinas de luz.

Em determinados períodos pode ser solicitada uma supressão intencional da função de proteção. O muting é uma supressão intencional e temporária da função de proteção. O chamado funcionamento muting é acionado por sensores muting (p. ex. durante o transporte de material para a área de perigo).

---

**Indicação**

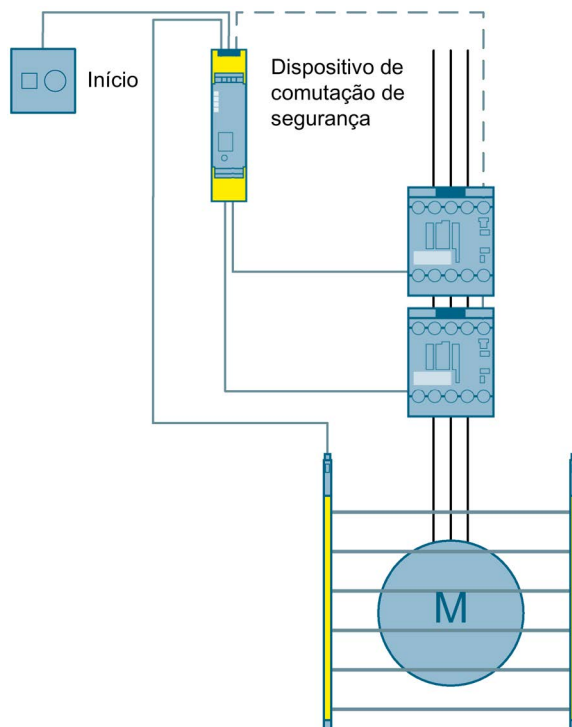
As cortinas de luz só conseguem cumprir o seu efeito protetor se forem montadas com uma distância de segurança suficiente. As fórmulas de cálculo para a distância de segurança dependem do tipo da proteção fusível. As situações de montagem e fórmulas de cálculo encontram-se na norma EN 13855 ("Disposição de instalações de proteção considerando as velocidades de aproximação de partes do corpo").

---

## 3.4.2 Monitoramento do acesso através de uma cortina de luz até SIL 3 ou PL e com um dispositivo de comutação de segurança

### Aplicação

Para monitorar o acesso a uma área de perigo aberta, é possível utilizar os chamados dispositivos de proteção que atuam sem contato, como por exemplo, uma cortina de luz. Quando o trajeto da luz é interrompido, é acionado um sinal de desativação.

### Estrutura

Esquema 3-20 Monitoramento do acesso através de uma cortina de luz até SIL 3 ou PL e com um dispositivo de comutação de segurança

## Modo de funcionamento

A cortina de luz é constituída por uma unidade emissora e por uma unidade receptora. Entre as duas encontra-se o campo de proteção. Se o trajeto de luz não for interrompido, as saídas OSSD1 e OSSD2 conduzem tensão e são avaliadas pelo dispositivo de comutação de segurança. Se o trajeto de luz for interrompido, as duas saídas desligam-se e o dispositivo de comutação de segurança abre os circuitos de liberação, provocando o desligamento seguro dos contatores de potência. A ligação pode ser feita novamente se o trajeto de luz não for interrompido e o circuito de retorno estiver fechado. Isso pode ser feito automaticamente ou através de um botão de arranque em função do aplicativo.

## Componentes relativos à segurança

| Cortina de luz | Dispositivo de comutação de segurança | Contator |
|---|---|---|
| | | |
| SICK C4000 | 3SK1 (http://www.siemens.com/safety-relays) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

## Ver também

Esquema elétrico e avaliação SET (http://support.automation.siemens.com/WW/view/pt/73136329)

### 3.4.3 Monitoramento do acesso através de uma cortina de luz até SIL 3 ou PL e com um sistema modular de segurança

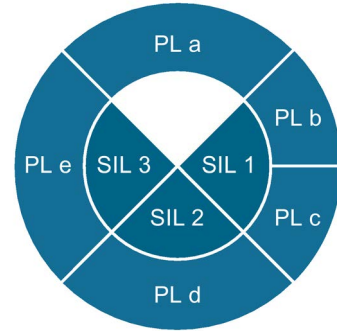
#### Aplicação

Para monitorar o acesso a uma área de perigo aberta, é possível utilizar os chamados dispositivos de proteção que atuam sem contato, como por exemplo, uma cortina de luz. Quando o trajeto da luz é interrompido, é acionado um sinal de desativação.

#### Estrutura

Esquema 3-21 Monitoramento do acesso através de uma cortina de luz até SIL 3 ou PL e com um sistema modular de segurança

## Modo de funcionamento

A cortina de luz é constituída por uma unidade emissora e por uma unidade receptora. Entre as duas encontra-se o campo de proteção. Se o trajeto de luz não for interrompido, as saídas OSSD1 e OSSD2 conduzem tensão e são avaliadas pelo sistema modular de segurança. Se o trajeto de luz for interrompido, as duas saídas desligam-se e o sistema modular de segurança abre os circuitos de liberação, provocando o desligamento seguro dos contatores de potência. A ligação pode ser feita novamente se o trajeto de luz não for interrompido e o circuito de retorno estiver fechado. Isso pode ser feito automaticamente ou através de um botão de arranque em função do aplicativo.

## Componentes relativos à segurança

| Cortina de luz | Sistema modular de segurança | Contator |
|---|---|---|
| | | |
| SICK C4000 | 3RK3 (http://www.siemens.com/sirius-mss) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

## Ver também

Esquema elétrico, projeto do sistema modular de segurança e avaliação SET (http://support.automation.siemens.com/WW/view/pt/69064070)

### 3.4.4 Monitoramento do acesso através de uma esteira sensível a pressão até SIL 3 ou PL e com um dispositivo de comutação de segurança

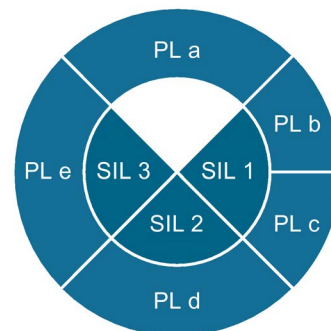
#### Aplicação

Para monitorar o acesso a uma área de perigo aberta, é possível utilizar esteiras sensíveis a pressão, que acionam um sinal de desativação quando são pisadas.

#### Estrutura

Esquema 3-22 Monitoramento do acesso através de uma esteira sensível a pressão até SIL 3 ou PL e com um dispositivo de comutação de segurança

## Modo de funcionamento

Com o dispositivo de comutação de segurança 3SK1 é possível avaliar esteiras sensíveis a pressão com base no princípio do contato de interrupção (ou contato de interrupção/contato de estabelecimento). Neste princípio, o circuito do sensor de dois canais é interrompido quando ocorre uma entrada. Por conseguinte, o dispositivo de comutação de segurança abre os circuitos de liberação, provocando o desligamento seguro dos contatores de potência. A ligação pode ser feita novamente se a esteira sensível a pressão estiver livre e o circuito de retorno estiver fechado. Isso pode ser feito automaticamente ou através de um botão de arranque em função do aplicativo.

## Componentes relativos à segurança

| Esteira sensível a pressão | Dispositivo de comutação de segurança | Contator |
|---|---|---|
| | | |
| | 3SK1 (http://www.siemens.com/safety-relays) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

## Ver também

Esquema elétrico e avaliação SET (http://support.automation.siemens.com/WW/view/pt/77262359)

### 3.4.5 Monitoramento do acesso através de uma esteira sensível a pressão até SIL 3 ou PL e com um sistema modular de segurança

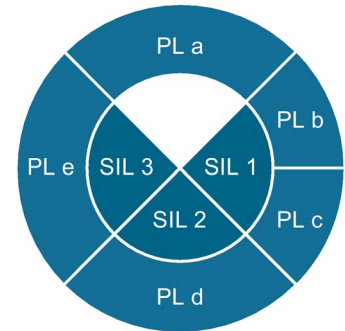
#### Aplicação

Para monitorar o acesso a uma área de perigo aberta, é possível utilizar esteiras sensíveis a pressão, que acionam um sinal de desativação quando são pisadas.

#### Estrutura

Esquema 3-23 Monitoramento do acesso através de uma esteira sensível a pressão até SIL 3 ou PL e com um sistema modular de segurança

## Modo de funcionamento

As esteiras sensíveis a pressão podem basear-se no princípio do contato de interrupção ou no princípio do circuito cruzado. No caso do princípio do contato de interrupção, o circuito do sensor de dois canais é interrompido quando ocorre uma entrada. Por outro lado, no caso do princípio do circuito cruzado, é acionado um circuito cruzado entre os dois circuitos de sensores quando ocorre uma entrada. Em ambos os casos, o sinal é avaliado pelo sistema modular de segurança. Por conseguinte, o sistema modular de segurança abre os circuitos de liberação, provocando o desligamento seguro dos contatores de potência. A ligação pode ser feita novamente se a esteira sensível a pressão estiver livre e o circuito de retorno estiver fechado. Isso pode ser feito automaticamente ou através de um botão de arranque em função do aplicativo.

## Componentes relativos à segurança

| Esteira sensível a pressão | Sistema modular de segurança | Contator |
|---|---|---|
| | | |
| | 3RK3 (http://www.siemens.com/sirius-mss) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

## Ver também

Esquema elétrico, projeto do sistema modular de segurança e avaliação SET (http://support.automation.siemens.com/WW/view/pt/77262361)

### 3.4.6 Monitoramento da área através de um scanner a laser até SIL 2 ou PL d com um dispositivo de comutação de segurança

#### Aplicação

Para monitorar o acesso não autorizado a áreas inteiras, são utilizados frequentemente scanners a laser. Estes monitoram amplamente uma área de perigo e acionam um sinal de desativação quando detectam objetos.

#### Estrutura

Esquema 3-24 Monitoramento da área através de um scanner a laser até SIL 2 ou PL d com um dispositivo de comutação de segurança

## Modo de funcionamento

O scanner a laser monitora amplamente uma zona de segurança. Geralmente, esta pode ser dividida numa área de aviso e numa área de perigo. Quando se entra na área de aviso é emitido um aviso de advertência, por exemplo, através de uma lâmpada de sinalização. Por outro lado, no caso de se entrar na zona de segurança a máquina é desligada.

Além disso, as saídas OSSD1 e OSSD2 conduzem tensão durante a operação e são avaliadas pelo dispositivo de comutação de segurança. Se o trajeto de luz for interrompido, as duas saídas desligam-se e o dispositivo de comutação de segurança abre os circuitos de liberação, provocando o desligamento seguro dos contatores de potência. A ligação pode ser feita novamente se o trajeto de luz não for interrompido e o circuito de retorno estiver fechado. Isso pode ser feito automaticamente ou através de um botão de arranque em função do aplicativo.

## Componentes relativos à segurança

| Scanner a laser | Dispositivo de comutação de segurança | Contator |
|---|---|---|
| | | |
| SICK S3000 | 3SK1 (http://www.siemens.com/safety-relays) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

## Ver também

Esquema elétrico e avaliação SET (http://support.automation.siemens.com/WW/view/pt/77262367)

### 3.4.7 Monitoramento da área através de um scanner a laser até SIL 2 ou PL d com um sistema modular de segurança

#### Aplicação

Para monitorar o acesso não autorizado a áreas inteiras, são utilizados frequentemente scanners a laser. Estes monitoram amplamente uma área de perigo e acionam um sinal de desativação quando detectam objetos.

#### Estrutura

Esquema 3-25 Monitoramento da área através de um scanner a laser até SIL 2 ou PL d com um sistema modular de segurança

## Modo de funcionamento

O scanner a laser monitora amplamente uma área de perigo. Geralmente, esta pode ser dividida numa área de aviso e numa zona de segurança. Quando se entra na área de aviso é emitido um aviso de advertência, por exemplo, através de uma lâmpada de sinalização. Por outro lado, no caso de se entrar na zona de segurança a máquina é desligada.

Além disso, as saídas OSSD1 e OSSD2 conduzem tensão durante a operação e são avaliadas pelo dispositivo de comutação de segurança. Se o trajeto de luz for interrompido, as duas saídas desligam-se e o dispositivo de comutação de segurança abre os circuitos de liberação, provocando o desligamento seguro dos contatores de potência. A ligação pode ser feita novamente se o trajeto de luz não for interrompido e o circuito de retorno estiver fechado. Isso pode ser feito automaticamente ou através de um botão de arranque em função do aplicativo.

## Componentes relativos à segurança

| Scanner a laser | Sistema modular de segurança | Contator |
|---|---|---|
| | | |
| SICK S3000 | 3RK3 (http://www.siemens.com/sirius-mss) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

### Ver também

Esquema elétrico, projeto do sistema modular de segurança e avaliação SET (http://support.automation.siemens.com/WW/view/pt/77284304)

## 3.5 Monitoramento seguro das rotações/paralisação

### 3.5.1 Introdução

Nas máquinas, cujos movimentos ou peças em movimento possam representar um perigo para as pessoas e para a máquina, é utilizado frequentemente um monitoramento das rotações/paralisação.

Frequentemente estes aplicativos são realizados em conjunto com instalações de proteção seccionadoras (porta de proteção) e retenção da porta de proteção.

Os dispositivos de travamento com retenção servem para proteger as áreas de perigo de acesso inadvertido. Isso geralmente tem dois motivos:

1. Para proteger as pessoas de movimentos subsequentes e perigosos da máquina, de elevadas temperaturas, etc.. Sobre este assunto, a ISO 14119 ou a EN 1088 fornece os princípios orientadores para a disposição e seleção de dispositivos de travamento. Nesta norma é requerido que a área de perigo só fique acessível após a parada dos movimentos perigosos da máquina.
2. Uma retenção pode fazer sentido por motivos da segurança do processo. Este caso verifica-se quando o perigo é excluído após a abertura da instalação de proteção mas ainda existe o risco de a máquina ou a peça ficar danificada. Aqui a máquina é primeiro deslocada para uma posição de parada adequada, antes de o acesso ser aprovado.

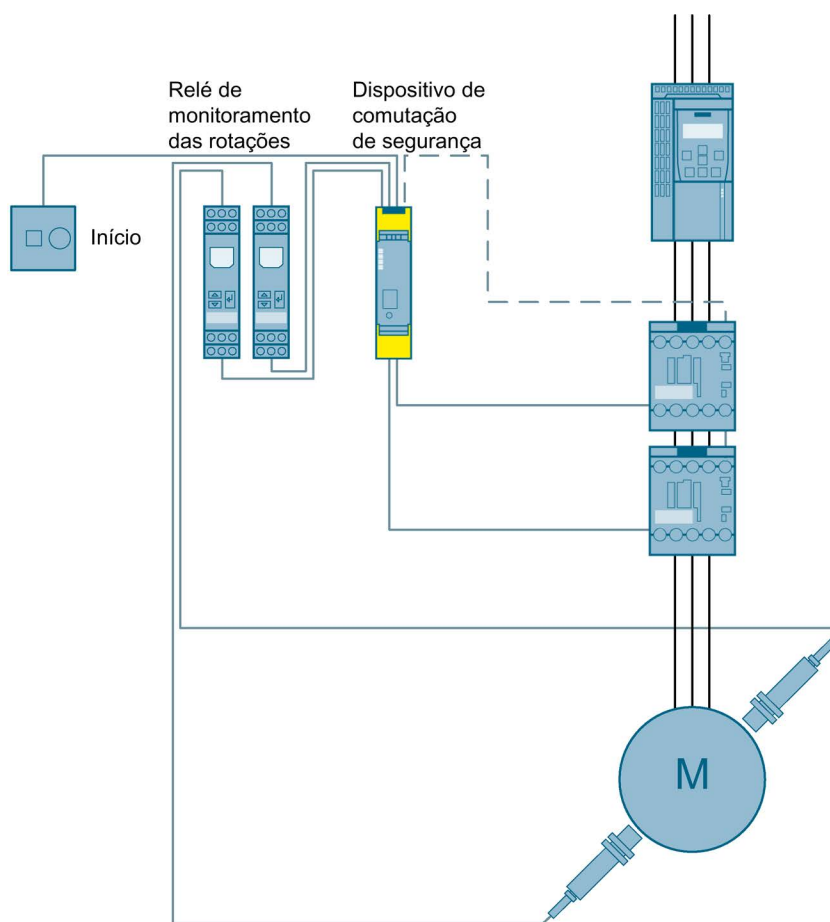
No monitoramento das rotações, a retenção da porta de proteção, p. ex., só é desbloqueada quando a peça em movimento fica imobilizada ou funciona com uma rotação segura.

Contrariamente ao monitoramento das rotações, no monitoramento da paralisação, p. ex., a retenção da porta de proteção só é desbloqueada depois de a paralisação ser alcançada.

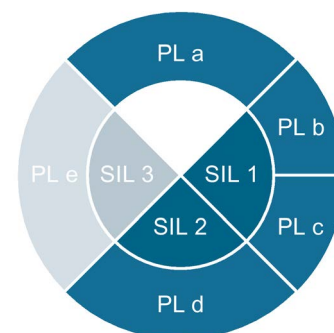
### 3.5.2 Monitoramento seguro das rotações até SIL 2 ou PL d com um dispositivo de comutação de segurança e um relé de monitoramento das rotações

#### Aplicação

Para assegurar que, mesmo em caso de falha, a rotação de um motor permanece limitada de forma a proteger as pessoas de eventuais quedas de peças de ferramentas, as rotações são monitoradas com a ajuda de dois relés de monitoramento das rotações e um dispositivo de comutação de segurança.

#### Estrutura

Esquema 3-26 Monitoramento seguro das rotações até SIL 2 ou PL d com um dispositivo de comutação de segurança e um relé de monitoramento das rotações

## Modo de funcionamento

Através da utilização redundante de dois relés de monitoramento das rotações padrão é possível alcançar até SIL 2 ou PL d. No processo, é definido nos dois relés de monitoramento das rotações um determinado limite das rotações ou uma determinada faixa de rotações (limite superior e limite inferior). Estes monitoram continuamente as rotações do motor e indicam se o limite ou a faixa das rotações foi mantido ou ultrapassado, através de contatos do relé.

Por sua vez, o dispositivo de comutação de segurança monitora os sinais do relé de monitoramento das rotações quanto a discrepância ou circuito cruzado.
Se as rotações do motor ultrapassarem o limite das rotações ou saírem da faixa de rotações, o motor é desligado imediatamente de forma segura.
É possível ligar novamente através do botão de arranque, se as rotações do motor tornarem a descer abaixo do limite das rotações ou se se encontrarem dentro da faixa de rotações ou ainda se se verificar a imobilização e o circuito de retorno estiver fechado.

---

### Indicação

Se forem utilizados dois relés de monitoramento redundantes no circuito do sensor para a detecção das grandezas do processo, poderá eventualmente suceder que um relé de monitoramento detecte uma ultrapassagem do valor limite primeiro que o outro. A razão para isso podem ser diferenças de ajuste e de medição dos aparelhos e dos sensores externos.

No exemplo referido em cima, seria possível um relé de monitoramento detectar a ultrapassagem do valor limite pouco antes do segundo, no caso de uma subida contínua das rotações. Neste caso, a alimentação de energia da unidade propulsora é desligada. As rotações descem de imediato. Devido à comparação cruzada necessária das entradas na avaliação relativa à segurança, permanece um erro de discrepância. Uma reativação do aplicativo só é possível após um retorno ao zero dos dois canais. Neste caso, é necessário verificar e resetar manualmente os relés de monitoramento.

Este comportamento pode ocorrer durante o monitoramento de grandezas do processo que aumentam lentamente. As possibilidades para evitar um erro de discrepância são, p. ex.:

- Apuramento empírico do parâmetro de ajuste para a sincronização do relé de monitoramento
- Estrutura idêntica dos sensores externos (sensores do mesmo tipo, com o mesmo comprimento de cabos, etc.)

---

## Componentes relativos à segurança

| Relé de monitoramento das rotações | Dispositivo de comutação de segurança | Contator |
|---|---|---|
| | | |
| 2x 3UG4651 (http://www.siemens.com/sirius-monitoring) | 3SK1 (http://www.siemens.com/safety-relays) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

## Ver também

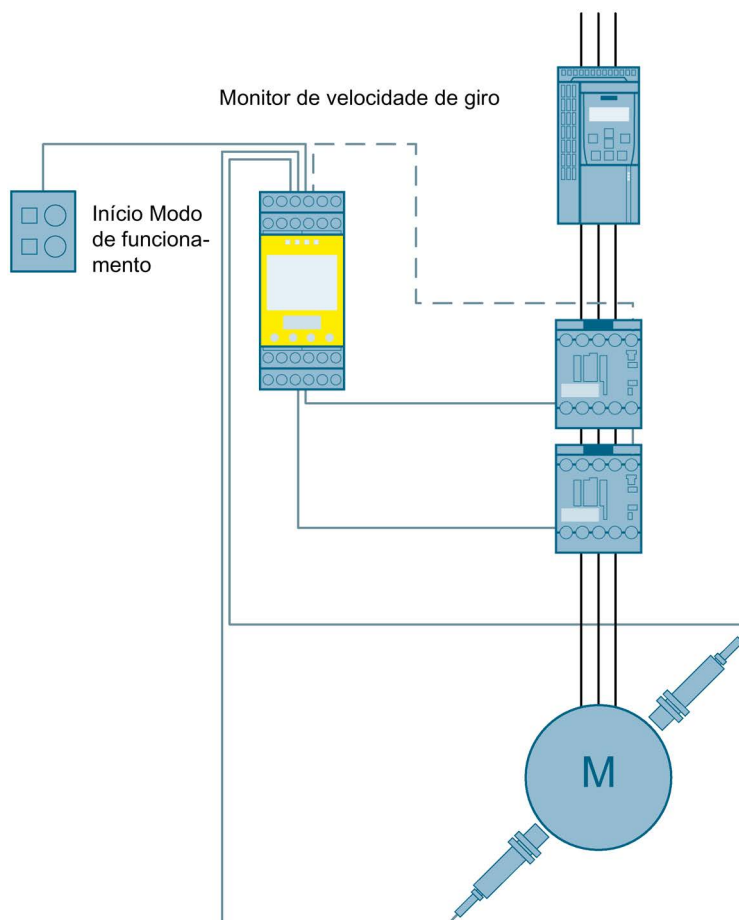
Esquema elétrico e cálculo SET
(http://support.automation.siemens.com/WW/view/pt/69065516)

Documento sobre a utilização de interruptores de segurança até SIL 2 ou PL d
(http://support.automation.siemens.com/WW/view/pt/35443942)

### 3.5.3 Monitoramento seguro das rotações até SIL 3 ou PL e com um monitor de velocidade de giro

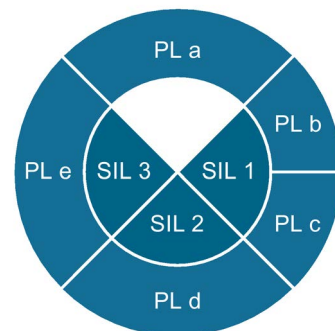
#### Aplicação

Para assegurar que, mesmo em caso de falha, a rotação de um motor permanece limitada de forma a proteger as pessoas de eventuais quedas de peças de ferramentas, as rotações são monitoradas com a ajuda de um monitor de velocidade de giro.

#### Estrutura

Esquema 3-27 Monitoramento seguro das rotações até SIL 3 ou PL e com um monitor de velocidade de giro

## Modo de funcionamento

No monitor de velocidade de giro é definido um determinado limite das rotações ou uma determinada faixa de rotações (limite superior e limite inferior).
É possível comutar entre o funcionamento de ajuste e o funcionamento automático com faixas individuais de rotações através de um seletor de modo de operação.
Se a respectiva faixa de rotações for ultrapassada ou não for alcançada, os contatores de potência são desligados de forma segura.

É possível ligar novamente através do botão de arranque, assim que os sistemas de atuadores se desligarem e o circuito de retorno estiver fechado.

## Componentes relativos à segurança

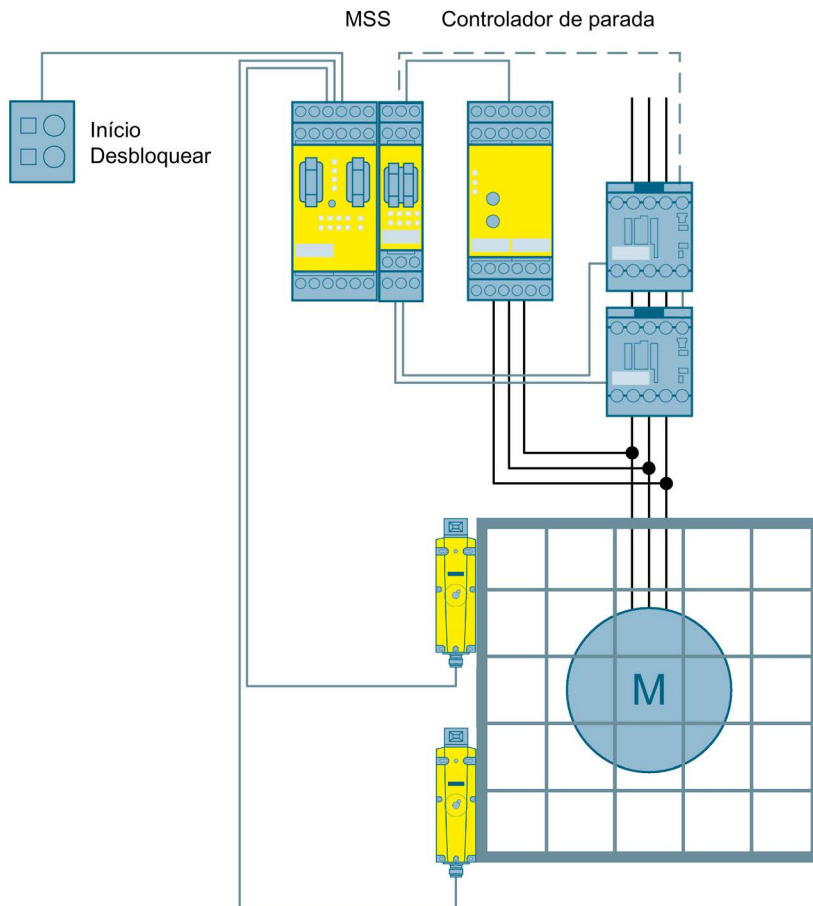
| Monitor de velocidade de giro | Contator |
|---|---|
| | |
| 3TK2810-1<br>(http://www.automation.siemens.com/mcms/industrial-controls/en/safety-systems/3tk28) | 2x 3RT20<br>(http://www.siemens.com/sirius-switching) |

## Ver também

Esquema elétrico e avaliação SET
(http://support.automation.siemens.com/WW/view/pt/69065043)

## 3.5.4 Monitoramento seguro da paralisação incl. retenção da porta de proteção até SIL 3 ou PL e com um sistema modular de segurança

### Aplicação

O sistema modular de segurança monitora uma porta de proteção. O controlador de parada assegura a interdição do acesso às peças da máquina em movimento e perigosas, durante o funcionamento do motor.

Esquema 3-28 Monitoramento seguro da paralisação incl. retenção da porta de proteção até SIL 3 ou PL e com um sistema modular de segurança

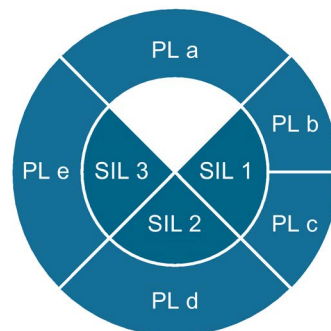
## Modo de funcionamento

O controlador de parada seguro 3TK2810-0 mede uma tensão induzida por magnetização residual do motor em funcionamento em três terminais do suporte de bobinagem. Se a tensão de indução tender para 0, tal é significativo para a parada do motor do aparelho e o relé de saída serem ativados.

O sistema modular de segurança monitora este sinal do controlador de parada bem como os dois interruptores de segurança.

Se for detectada uma parada do motor e o botão para desbloquear for ligado, a retenção é desbloqueada e a porta de proteção pode ser aberta. Ao mesmo tempo, os contatores são desligados de modo seguro evitando assim um rearranque inadvertido do motor.

É possível ligar novamente através do botão de arranque, se a porta estiver bloqueada e o circuito de retorno estiver fechado.

O desligar em caso de emergência apresenta uma função de segurança adicional que não será mais abordada.

## Componentes relativos à segurança

| Interruptor de segurança com retenção | Controlador de parada | Sistema modular de segurança | Módulo de expansão | Contator |
|---|---|---|---|---|
| 2x 3SE5 (http://www.siemens.com/sirius-detecting) | 3TK2810-0 (http://www.automation.siemens.com/mcms/industrial-controls/en/safety-systems/3tk28) | 3RK3 (http://www.siemens.com/sirius-mss) | 3RK3 (http://www.siemens.com/sirius-mss) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

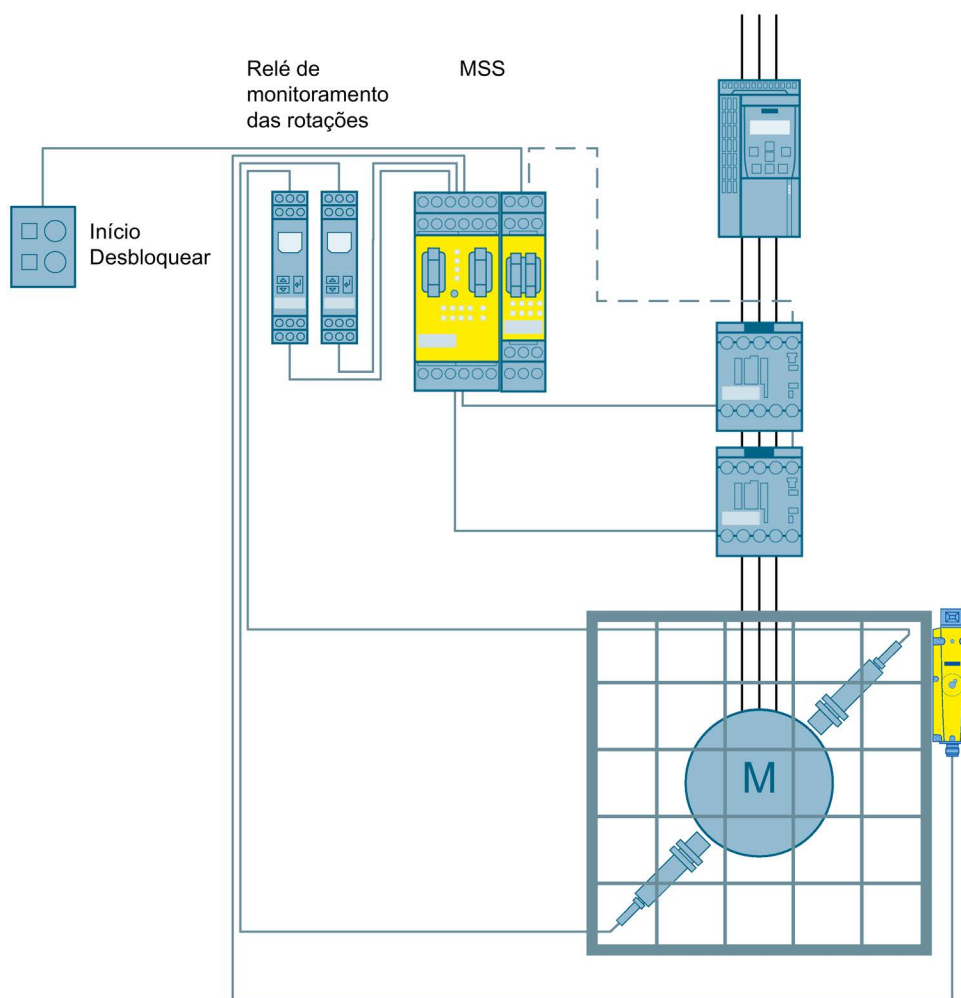
## Ver também

Esquema elétrico, projeto do sistema modular de segurança e avaliação SET (http://support.automation.siemens.com/WW/view/pt/69065515)

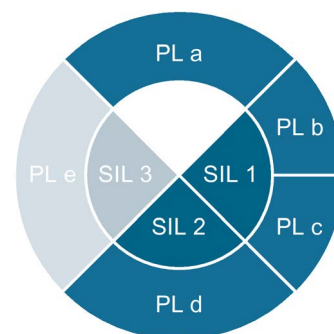
### 3.5.5 Monitoramento seguro das rotações, da porta de proteção e da retenção até SIL 2 ou PL d com um sistema modular de segurança e um relé de monitoramento das rotações

#### Aplicação

O sistema modular de segurança assegura, com a ajuda do relé de monitoramento das rotações, que a partir de uma rotação ajustável, não será permitido qualquer acesso às peças da máquina em movimento e perigosas.

#### Estrutura

Esquema 3-29 Monitoramento seguro das rotações, da porta de proteção e da retenção até SIL 2 ou PL d com um sistema modular de segurança e um relé de monitoramento das rotações

## Modo de funcionamento

Através da utilização redundante de dois relés de monitoramento das rotações padrão é possível alcançar até SIL 2 ou PL d. Para o efeito, é definida uma faixa de rotações segura no relé de monitoramento das rotações. Enquanto as rotações se encontrarem fora desta faixa segura, o acesso às peças da máquina em movimento e perigosas é impedido através de uma porta de proteção com retenção. O sistema modular de segurança monitora os sinais do relé de monitoramento das rotações bem como os dois interruptores de segurança.

Enquanto as rotações do motor se encontrarem dentro da faixa de rotações segura, é possível desbloquear a retenção através do botão de desbloqueio e abrir a porta de proteção. Se as rotações do motor ultrapassarem a faixa de rotações segura enquanto a porta estiver aberta, o motor é desligado de imediato de forma segura. É possível ligar novamente através do botão de arranque, se a porta estiver bloqueada e o circuito de retorno estiver fechado.

Neste exemplo, a função de segurança "Monitoramento da porta de proteção" e a função de segurança "Retenção da porta de proteção" foram concebidas até SIL 2 ou PL d.

Considerando as exclusões de falhas, é permitida a utilização de apenas um interruptor de segurança com ou sem retenção até SIL 2 ou PL d. Para mais informações consulte o documento referido em baixo.

---

### Indicação

Se forem utilizados dois relés de monitoramento redundantes no circuito do sensor para a detecção das grandezas do processo, poderá eventualmente suceder que um relé de monitoramento detecte uma ultrapassagem do valor limite primeiro que o outro. A razão para isso podem ser diferenças de ajuste e de medição dos aparelhos e dos sensores externos.

No exemplo referido em cima, seria possível um relé de monitoramento detectar a ultrapassagem do valor limite pouco antes do segundo, no caso de uma subida contínua das rotações. Neste caso, a alimentação de energia da unidade propulsora é desligada. As rotações descem de imediato. Devido à comparação cruzada necessária das entradas na avaliação relativa à segurança, permanece um erro de discrepância. Uma reativação do aplicativo só é possível após um retorno ao zero dos dois canais. Neste caso, é necessário verificar e resetar manualmente os relés de monitoramento.

Este comportamento pode ocorrer durante o monitoramento de grandezas do processo que aumentam lentamente. As possibilidades para evitar um erro de discrepância são, p. ex.:

- Apuramento empírico do parâmetro de ajuste para a sincronização do relé de monitoramento
- Estrutura idêntica dos sensores externos (sensores do mesmo tipo, com o mesmo comprimento de cabos, etc.)

---

## Componentes relativos à segurança

| Interruptor de segura-nça com retenção | Relé de monitoramen-to das rotações | Sistema modular de segurança | Módulo de expansão | Contator |
|---|---|---|---|---|
| | | | | |
| 3SE5 (2 canais) (http://www.siemens.com/sirius-detecting) | 2x 3UG4651 (http://www.siemens.com/sirius-monitoring) | 3RK3 (http://www.siemens.com/sirius-mss) | 3RK3 (http://www.siemens.com/sirius-mss) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

### Ver também

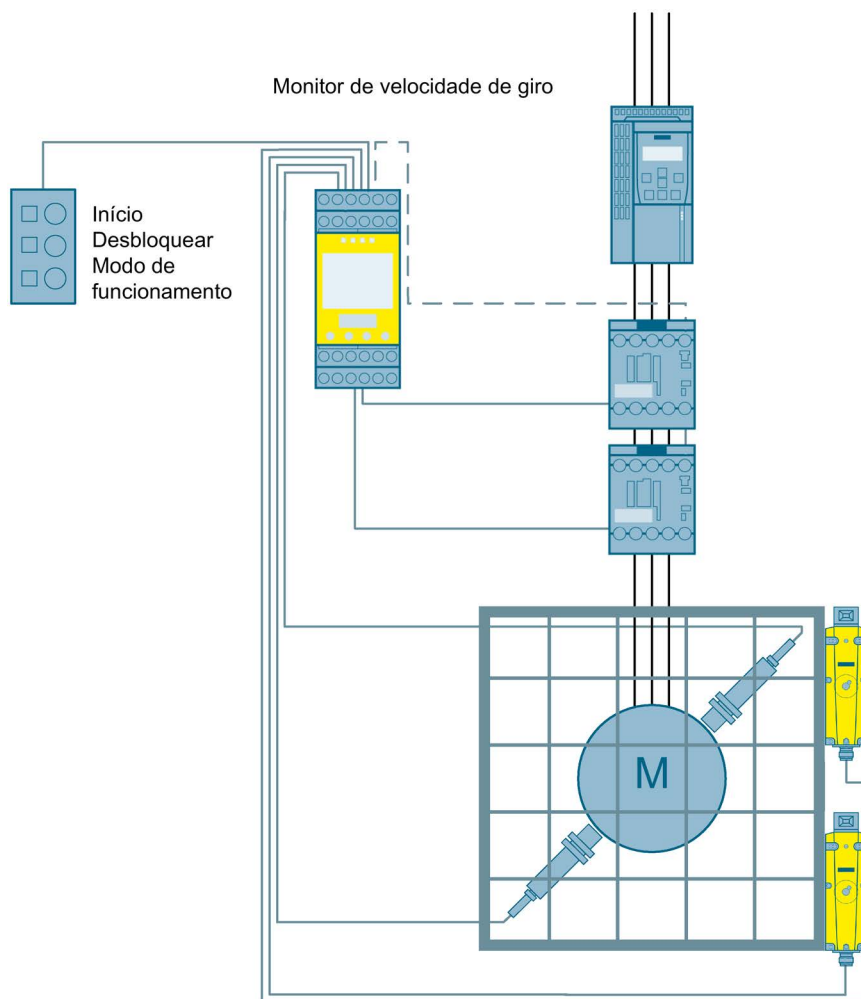
Esquema elétrico, projeto do sistema modular de segurança e avaliação SET (http://support.automation.siemens.com/WW/view/pt/77284310)

Documento sobre a utilização de interruptores de segurança até SIL 2 ou PL d (http://support.automation.siemens.com/WW/view/pt/35443942)

### 3.5.6 Monitoramento seguro das rotações, da porta de proteção e da retenção até SIL 3 ou PL e com um monitor de velocidade de giro

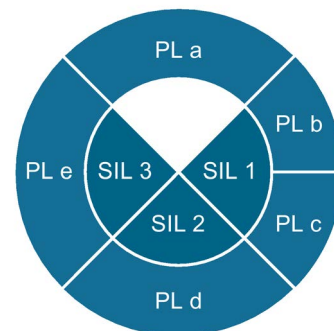
#### Aplicação

O monitor de velocidade de giro assegura que a partir de uma rotação ajustável, não será permitido qualquer acesso às peças da máquina em movimento e perigosas.

#### Estrutura

Esquema 3-30 Monitoramento seguro das rotações, da porta de proteção e da retenção até SIL 3 ou PL e com um monitor de velocidade de giro

## Modo de funcionamento

No monitor de velocidade de giro é definida uma faixa de rotações segura. Enquanto as rotações se encontrarem fora desta faixa segura, o acesso às peças da máquina em movimento e perigosas é impedido através de uma porta de proteção com retenção. O monitor de velocidade de giro monitora em simultâneo a posição da porta de proteção.

É possível comutar entre o funcionamento de ajuste e o funcionamento automático com faixas individuais de rotações através de um seletor de modo de operação. A detecção de uma paralisação e a manutenção do valor dentro da faixa de rotações definida são emitidas através de duas saídas do relé

No funcionamento automático a porta de proteção permanece bloqueada, enquanto não for detectada uma paralisação. Se a faixa de rotações no modo automático for ultrapassada ou não for alcançada, os contatores de potência são desligados de forma segura.
No modo de ajuste, a porta de proteção está permanentemente liberada. Se a faixa de rotações no modo de ajuste for ultrapassada ou não for alcançada, os contatores de potência são desligados.

Se a porta de proteção estiver aberta, o monitor de velocidade de giro assegura que o motor não possa ser ligado. É possível ligar novamente através do botão de arranque, se a porta e o circuito de retorno estiverem fechados.

## Componentes relativos à segurança

| Interruptor de segurança com retenção | Monitor de velocidade de giro | Contator |
|---|---|---|
| | | |
| 2x 3SE5 (http://www.siemens.com/sirius-detecting) | 3TK2810-1 (http://www.automation.siemens.com/mcms/industrial-controls/en/safety-systems/3tk28) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

## Ver também

Esquema elétrico e avaliação SET
(http://support.automation.siemens.com/WW/view/pt/77284316)

# 3.6 Operação segura

## 3.6.1 Introdução

Se um operador tiver de manusear uma máquina numa área de perigo, p. ex. para colocar ou retirar peças de prensas, máquinas de corte ou máquinas semelhantes, é necessário implementar funções de segurança para que a máquina possa ser operada de forma segura. O início de um movimento perigoso só pode ocorrer, p. ex., quando o operador não tiver qualquer parte do corpo dentro da área de perigo. Uma possibilidade de isto ser assegurado é a utilização da operação com duas mãos. Neste caso, o operador tem de ligar um botão quase em simultâneo com as duas mãos, para iniciar a máquina ou o movimento perigoso. Quando o botão é solto, a máquina ou o movimento é parado.

O capítulo seguinte contém exemplos de aplicativos com operação com duas mãos para a operação segura da máquina.

---

**Indicação**

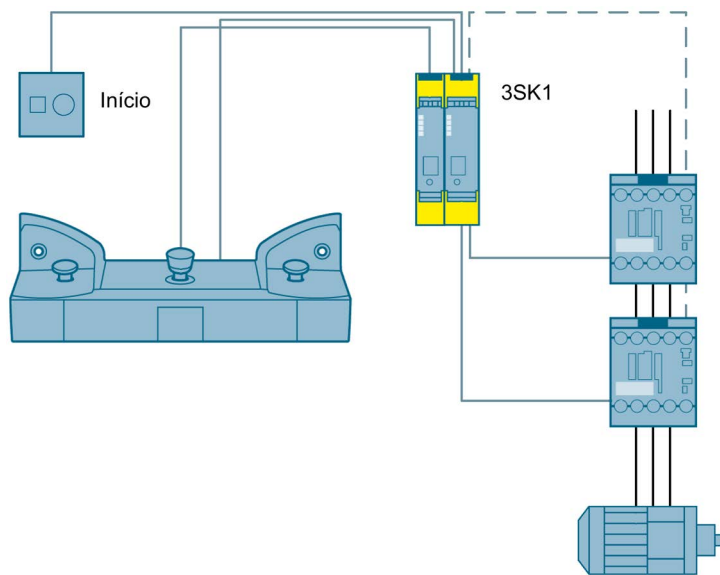
A seleção de um comando bimanual como dispositivo de segurança adequado depende da avaliação de riscos.

---

### 3.6.2 Operação com duas mãos até SIL 3 ou PL e com um dispositivo de comutação de segurança

#### Aplicação

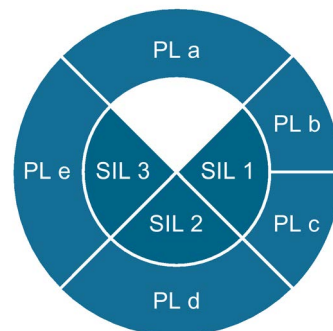
Os painéis de comando para duas mãos são compostos por dois botões que têm de ser acionados em simultâneo, para operar uma máquina. Desta forma é evitado que o operador possa intervir na área de perigo durante o funcionamento.

#### Estrutura

Esquema 3-31 Operação com duas mãos até SIL 3 ou PL e com um dispositivo de comutação de segurança

## Modo de funcionamento

Mediante a condição do acionamento em simultâneo dos dois botões, o operador fica ligado ao painel de comando para duas mãos e não pode intervir na área de perigo. O dispositivo de comutação de segurança só liga os circuitos de liberação quando os dois sinais ocorrem dentro de 500 ms e o circuito de retorno se encontra fechado.

Quando um dos dois botões é solto, o dispositivo de comutação de segurança desliga de imediato a máquina de forma segura.

Depois do acionamento da parada de emergência, só é possível ligar novamente através do botão de arranque.

## Componentes relativos à segurança

| Painel de comando para duas mãos | Dispositivo de comutação de segurança | Expansão da entrada | Contator |
|---|---|---|---|
| 3SB38 (http://www.siemens.com/sirius-commanding) | 3SK1 (http://www.siemens.com/safety-relays) | 3SK1 (http://www.siemens.com/safety-relays) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

## Ver também

Esquema elétrico e avaliação SET
(http://support.automation.siemens.com/WW/view/pt/74562494)

## 3.6.3 Operação com duas mãos até SIL 3 ou PL e com um sistema modular de segurança

### Aplicação

Os painéis de comando para duas mãos são compostos por dois botões que têm de ser acionados em simultâneo, para operar uma máquina. Desta forma é evitado que o operador possa intervir na área de perigo durante o funcionamento.

### Estrutura

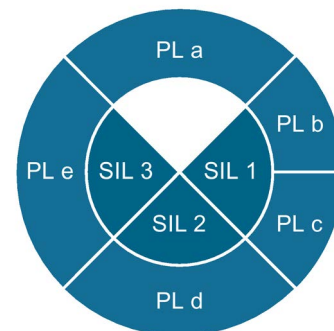
Esquema 3-32 Operação com duas mãos até SIL 3 ou PL e com um sistema modular de segurança

## Modo de funcionamento

Mediante a condição do acionamento em simultâneo dos dois botões, o operador fica ligado ao painel de comando para duas mãos e não pode intervir na área de perigo. O sistema modular de segurança só liga os circuitos de liberação quando os dois sinais ocorrem dentro de 500 ms e o circuito de retorno se encontra fechado.

Quando um dos dois botões é solto, o sistema modular de segurança desliga de imediato a máquina de forma segura.

Através de uma montagem de quatro canais no painel de comando para duas mãos é assegurado que a possível soldagem de um dos contatos é detectada de imediato.

Após o acionamento do aparelho de comando de parada de emergência, só é possível ligar novamente através do botão de arranque.

## Componentes relativos à segurança

| Painel de comando para duas mãos | Sistema modular de segurança | Contator |
|---|---|---|
| | | |
| 3SB38 (http://www.siemens.com/sirius-commanding) | 3RK3 (http://www.siemens.com/sirius-mss) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

## Ver também

Esquema elétrico, projeto do sistema modular de segurança e avaliação SET (http://support.automation.siemens.com/WW/view/pt/69064071)

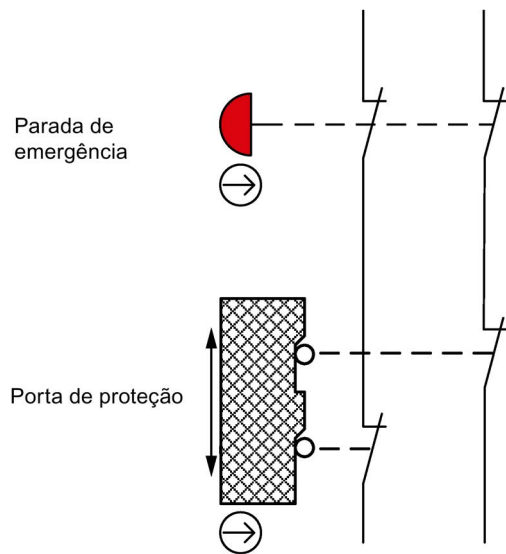
# 3.7 Combinações típicas de várias funções de segurança

## 3.7.1 Introdução

Em casos muito raros, é suficiente implementar apenas uma função de segurança numa máquina. Frequentemente são implementadas numa máquina várias funções de segurança em simultâneo (funções essas referidas nos capítulos anteriores), para que seja alcançada a segurança necessária.

Nos capítulos seguintes são mostrados exemplos de aplicativos que contêm combinações típicas de funções de segurança.

### Condições para a ligação em série de aparelhos de comando de parada de emergência e monitoramento da porta de proteção com interruptores de posição

Os aparelhos de comando de parada de emergência e os interruptores de posição podem ser ligados em série até PL d (segundo ISO 13849) ou SIL 2 (segundo IEC 62061), se for possível excluir que o aparelho de comando de parada de emergência e a porta de proteção não são acionados em simultâneo (caso contrário, não é possível ocorrer uma detecção de erros).

## Acoplamento ou cascata energética de funções de segurança

Se for necessário acoplar duas ou várias partes da instalação, ou seja, a solicitação de uma função de segurança a uma parte da instalação ativa a solicitação de uma função de segurança a outra parte da instalação, a transmissão do sinal tem de satisfazer as mesmas solicitações da função de segurança para a parte da instalação em questão.

### Exemplo:

Nas duas partes da instalação é monitorado um aparelho de comando de parada de emergência. A função de paragem de emergência na parte da instalação 1 está concebida segundo SIL 3 ou PL e e na parte da instalação 2 segundo SIL 2 ou PL d.

Enquanto que um comando de paragem de emergência, ativado na parte da instalação 2, tem efeito apenas nesta parte da instalação, um comando de parada de emergência, ativado na parte da instalação 1, deve imobilizar de forma segura as duas partes da instalação.

Como a avaliação de riscos para a parte da instalação 2 requer um SIL 2 ou PL d, é necessário que a transmissão do sinal do comando de parada de emergência da parte da instalação 1 corresponda no mínimo a este nível de segurança. Assim, os cabos de sinal têm de ser dispostos à prova de circuito transversal ou o sinal tem de ser transmitido através de uma comunicação segura (por exemplo ASIsafe).

Por princípio, a área de perigo tem de ser bem visível da posição a partir da qual é dado o comando de início/rearranque. A questão de saber se cada parte da instalação necessita de um botão de arranque próprio, depende da instalação e da avaliação de riscos.

---

### Indicação

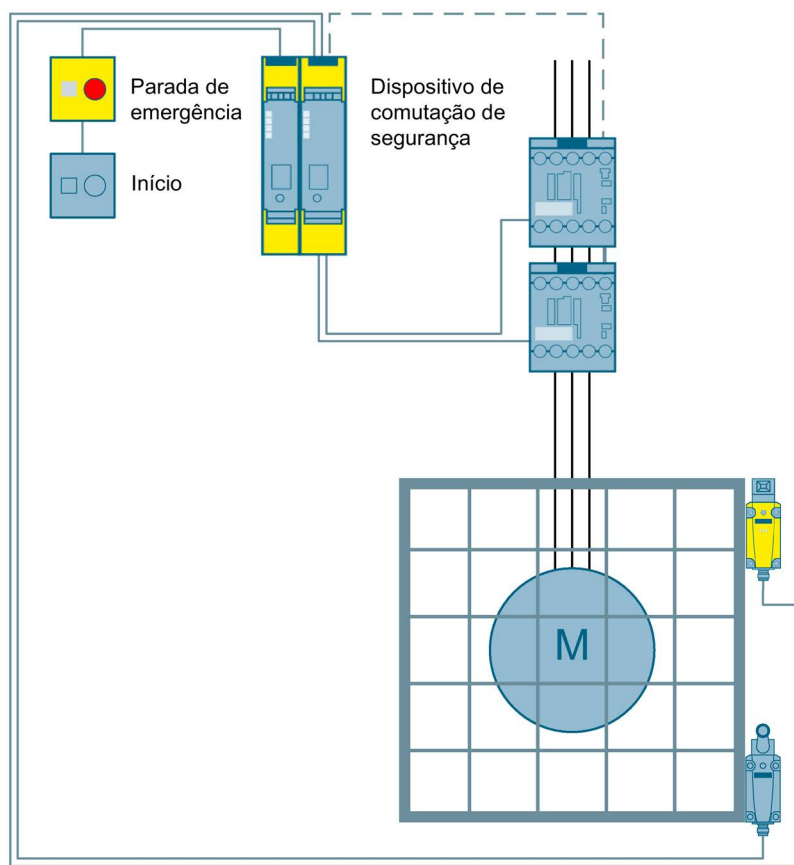
O acoplamento dentro de um armário de distribuição pode ser realizado em 1 canal, o que é permitido até SIL 3 ou PL e, pois a instalação de cabos dentro de um armário de distribuição é válida como sendo à prova de circuito P/resistente a curto-circuitos (exclusão de falhas segundo ISO 13849-2).

---

## 3.7.2 Monitoramento da parada de emergência e da porta de proteção até SIL 3 ou PL e com um dispositivo de comutação de segurança

### Aplicação

Para a delimitação de áreas de perigo são utilizadas frequentemente portas de proteção. Estas são monitoradas quanto à sua posição e, se necessário, é desligada a área da qual advém o perigo. Adicionalmente, para desligar a máquina em caso de emergência, é monitorado um aparelho de comando de parada de emergência.

### Estrutura

Esquema 3-33 Monitoramento da parada de emergência e da porta de proteção até SIL 3 ou PL e com um dispositivo de comutação de segurança

## Modo de funcionamento

O dispositivo de comutação de segurança monitora os dois interruptores de segurança bem como os dois contatos de parada de emergência através de uma expansão de entrada adicional. Com a ligação do aparelho de comando de parada de emergência ou com a abertura da porta de proteção, o dispositivo de comutação de segurança abre os circuitos de liberação e desliga de modo seguro os contatores de potência.

É possível ligar novamente através do botão de arranque, se a porta estiver fechada, o aparelho de comando de parada de emergência desbloqueado e o circuito de retorno fechado.

## Componentes relativos à segurança

| Aparelho de comando de parada de emergência | Interruptor de posição | Dispositivo de comutação de segurança | Expansão da entrada | Contator |
|---|---|---|---|---|
| 3SB3 (2 canais) (http://www.siemens.com/sirius-commanding) | 2x 3SE5 (http://www.siemens.com/sirius-detecting) | 3SK1 (http://www.siemens.com/safety-relays) | 3SK1 (http://www.siemens.com/safety-relays) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

## Ver também

Esquema elétrico e avaliação SET (http://support.automation.siemens.com/WW/view/pt/74562495)

### 3.7.3 Monitoramento da parada de emergência e da porta de proteção até SIL 3 ou PL e com um sistema modular de segurança

#### Aplicação

Para a delimitação de áreas de perigo são utilizadas frequentemente portas de proteção. Estas são monitoradas quanto à sua posição e, se necessário, é desligada a área da qual advém o perigo. Adicionalmente, para desligar a máquina em caso de emergência, é monitorado um aparelho de comando de parada de emergência.

#### Estrutura

Esquema 3-34 Monitoramento da parada de emergência e da porta de proteção até SIL 3 ou PL e com um sistema modular de segurança

## Modo de funcionamento

O sistema modular de segurança monitora os dois interruptores de segurança bem como o aparelho de comando de parada de emergência em dois canais. Com a ligação do aparelho de comando de parada de emergência ou com a abertura da porta de proteção, o sistema modular de segurança abre os circuitos de liberação e desliga de modo seguro os contatores de potência.

É possível ligar novamente através do botão de arranque, se a porta estiver fechada, o aparelho de comando de parada de emergência desbloqueado e o circuito de retorno fechado.

## Componentes relativos à segurança

| Aparelho de comando de parada de emergência | Interruptor de posição | | Sistema modular de segurança | Contator |
|---|---|---|---|---|
| | | | | |
| 3SB3 (2 canais) (http://www.siemens.com/sirius-commanding) | 2x 3SE5 (http://www.siemens.com/sirius-detecting) | | 3RK3 (http://www.siemens.com/sirius-mss) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

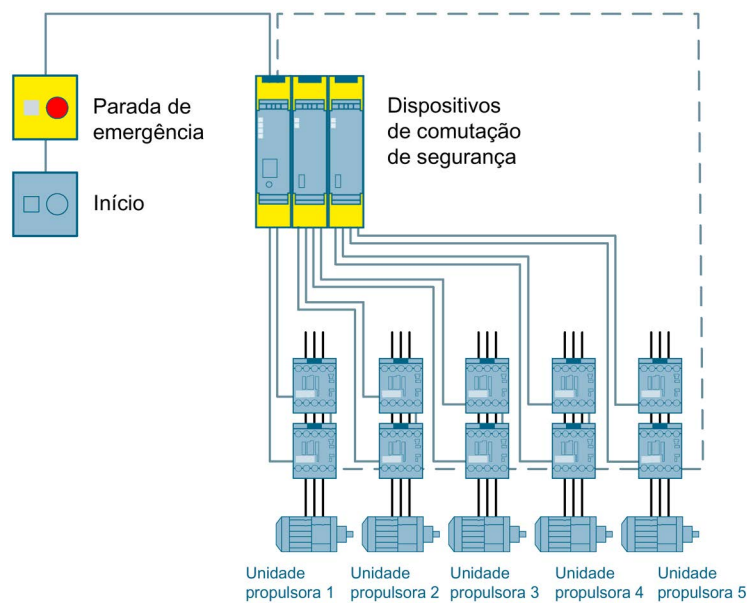
## Ver também

Esquema elétrico, projeto do sistema modular de segurança e avaliação SET (http://support.automation.siemens.com/WW/view/pt/74563943)

## 3.7.4 Desligamento de parada de emergência de vários motores até SIL 3 ou PL e com um dispositivo de comutação de segurança

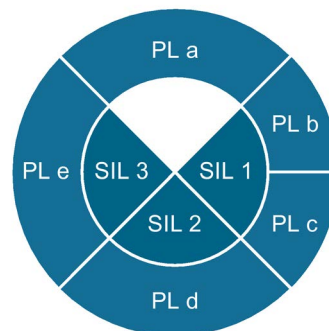
### Aplicação

Se for necessário desligar em simultâneo várias unidades propulsoras devido a um requisito de segurança (p. ex. carro da máquina, ferramenta da máquina, dispositivo de aspiração, etc.), tal pode ser feito com a ajuda de expansões de saída com circuitos de liberação adicionais.

### Estrutura

Esquema 3-35 Desligamento de parada de emergência de vários motores até SIL 3 ou PL e com um dispositivo de comutação de segurança

## Modo de funcionamento

O dispositivo de comutação de segurança monitora o aparelho de comando de parada de emergência em dois canais. Quando o aparelho de comando de parada de emergência é ligado, o dispositivo de comutação de segurança e as expansões de saída abrem os circuitos de liberação e desligam de modo seguro os contatores de potência. É possível ligar novamente através do botão de arranque, se o aparelho de comando de parada de emergência estiver desbloqueado e o circuito de retorno de todos os atuadores fechado.

O desligamento das unidades propulsoras individuais apresenta uma função de segurança própria, mesmo quando a ordem de desligamento provém do mesmo aparelho de comando de parada de emergência e dispositivo de comutação de segurança.

## Componentes relativos à segurança

| Aparelho de comando de parada de emergência | Dispositivo de comutação de segurança | Extensão de saída | Contator |
|---|---|---|---|
| | | | |
| 3SB3 (2 canais) (http://www.siemens.com/sirius-commanding) | 3SK1 (http://www.siemens.com/safety-relays) | 3SK1 (http://www.siemens.com/safety-relays) | 3RT20 (http://www.siemens.com/sirius-switching) |

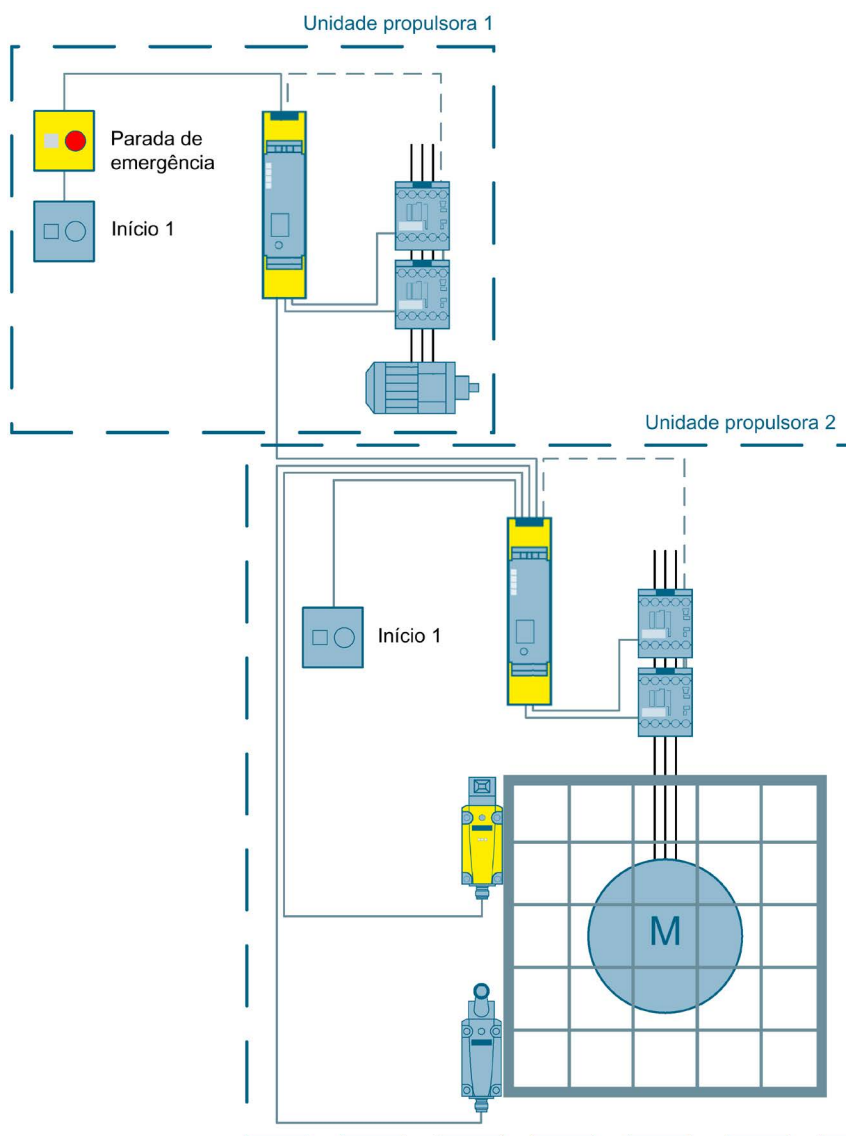
## Ver também

Esquema elétrico e avaliação SET (http://support.automation.siemens.com/WW/view/pt/74563681)

### 3.7.5 Cascata energética e dispositivos de comutação de segurança até SIL 3 ou PL e

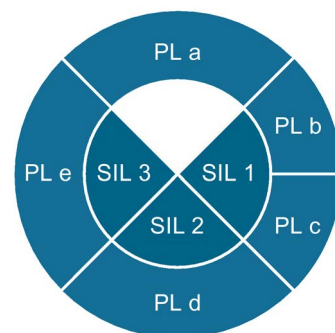
#### Aplicação

A cascata energética de dispositivos de comutação de segurança serve para ligar em série vários dispositivos de comutação de segurança. Desta forma, é possível encadear logicamente várias funções de segurança com um caminho de desativação comum. Ao mesmo tempo, é possível criar vários circuitos de liberação para um desligamento seletivo de elementos de acionamento.

#### Estrutura

Esquema 3-36 Cascata energética e dispositivos de comutação de segurança até SIL 3 ou PL e

## Modo de funcionamento

Os dois dispositivos de comutação de segurança apresentados estão interligados através da entrada em cascata. Se a parada de emergência for ativada no primeiro dispositivo de comutação de segurança, os dois dispositivos de comutação de segurança desligam consequentemente os seus atuadores. Por outro lado, com a abertura da tampa de proteção apresentada, por exemplo, só são desligados os sistemas de atuadores que se encontram por trás.

Se uma parada de emergência tiver sido ativada através do dispositivo de comutação de segurança hierarquicamente superior, o dispositivo de comutação subordinado tem de ser ligado manualmente através do botão de arranque. Um botão de arranque global só é possível se todas as áreas de perigo forem visíveis a partir deste botão de arranque.

### Indicação

Este exemplo aplica-se para a montagem dentro de um armário de distribuição. Se os dois dispositivos de comutação de segurança não se encontrarem no mesmo armário de distribuição, devem ser tomadas outras precauções, como por exemplo uma instalação à prova de circuito transversal do sinal em cascata.

## Componentes relativos à segurança

| Aparelho de comando de parada de emergência | Interruptor de segurança | Dispositivo de comutação de segurança | Contator |
|---|---|---|---|
| | | | |
| 3SB3 (2 canais) (http://www.siemens.com/sirius-commanding) | 2x 3SE5 (http://www.siemens.com/sirius-detecting) | 3SK1 (http://www.siemens.com/safety-relays) | 2x 3RT20 (http://www.siemens.com/sirius-switching) |

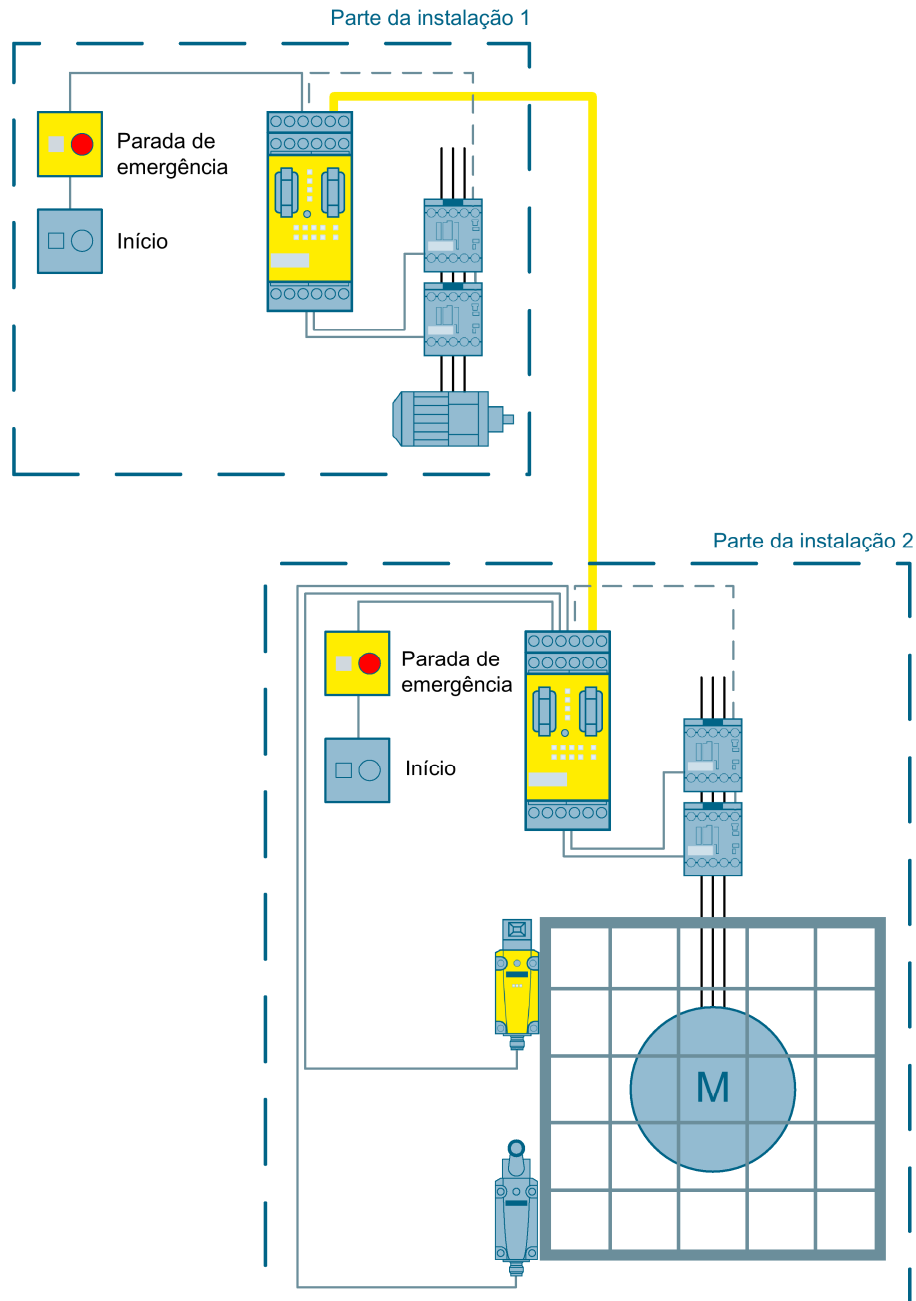
## Ver também

Esquema elétrico e avaliação SET
(http://support.automation.siemens.com/WW/view/pt/77282496)

### 3.7.6 Comunicação cruzada segura entre várias partes da instalação até SIL 3 ou PL e através de AS-i

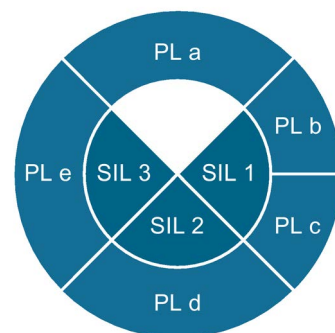
#### Aplicação

Para encadear logicamente várias partes da instalação umas com as outras, é necessária uma comunicação cruzada. Esta deve ser concebida failsafe, de forma a também transmitir sinais de desativação seguros. O sistema modular de segurança oferece esta possibilidade com AS-i.

#### Estrutura

Esquema 3-37 Comunicação cruzada segura entre várias partes da instalação até SIL 3 ou PL e através de AS-i

## Modo de funcionamento

As duas partes da instalação são dependentes uma da outra devido ao processo. Se for iniciado um desligamento da máquina numa das duas partes da instalação, esta ordem de desligamento é encaminhada para a outra parte da instalação através da comunicação cruzada segura pelo AS-i no sistema modular de segurança.

Adicionalmente também podem ser trocadas informações de diagnóstico e sinais de sinalização entre as duas partes da instalação.

### Indicação

A questão de saber se as duas partes da instalação podem ser novamente ligadas com um botão de arranque ou se é necessário um botão de arranque próprio para cada parte da instalação, depende da instalação e da avaliação de riscos.

## Componentes relativos à segurança

| Aparelho de comando de parada de emergência | Interruptor de segurança | Sistema modular de segurança | Contator |
|---|---|---|---|
| 2x 3SB3 (2 canais) (http://www.siemens.com/sirius-commanding) | 2x 3SE5 (http://www.siemens.com/sirius-detecting) | 2x 3RK3 (http://www.siemens.com/sirius-mss) | 4x 3RT20 (http://www.siemens.com/sirius-switching) |

### Indicação

Adicionalmente aos componentes relativos à segurança, é necessário um AS-i-Master e um elemento de rede AS-i para operar uma rede AS-i.

## Ver também

Projeto do sistema modular de segurança e avaliação SET (http://support.automation.siemens.com/WW/view/pt/88823146)

FAQs detalhadas sobre o tema: Comunicação cruzada segura (http://support.automation.siemens.com/WW/view/pt/58512565)

# Prescrições e normas 4

## 4.1 Prescrições e normas na União Europeia (UE)

### 4.1.1 Segurança de máquinas na Europa

#### 4.1.1.1 Bases jurídicas

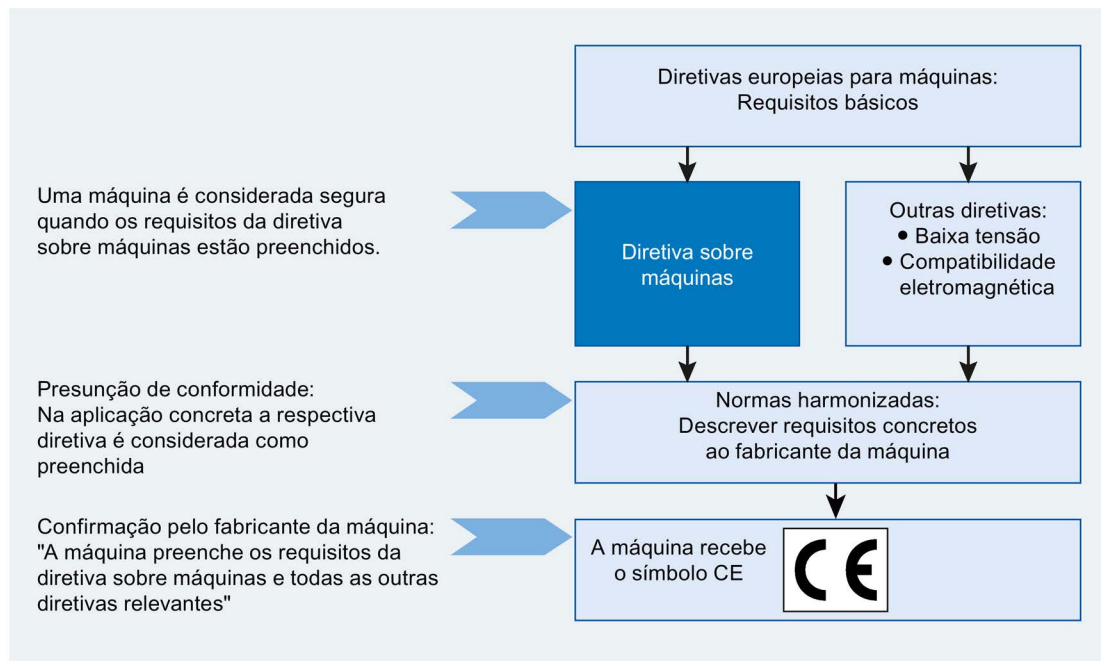
**Diretiva sobre máquinas (2006 / 42 / CE)**

Com a introdução do mercado único europeu foi decidida a harmonização das normas e prescrições nacionais de todos os estados-membros respeitantes à realização técnica de máquinas. Isso originou que a diretiva sobre máquinas teve que ser integrada na legislação nacional como uma diretiva relativa ao mercado interno por cada estado-membro. Na Alemanha, o conteúdo da diretiva sobre máquinas foi integrado como 9.º regulamento da legislação relativa à segurança de produtos (9. ProdSV). Isso sucedeu na diretiva sobre máquinas antes do reforço dos objetivos comuns de proteção, com a finalidade de suprimir barreiras técnicas ao comércio. A área de aplicação da diretiva sobre máquinas é muito vasta, conforme a sua definição "Máquina é um todo de peças e dispositivos interligados, dos quais pelo menos um é móvel". A área de aplicação abrange, para além disso, os equipamentos substituíveis, componentes de segurança, acessórios de elevação, correntes, cintos, cabos, veios articulados amovíveis e quase-máquinas.

Como "Máquina" também é designado um todo de máquinas, que, para que funcionem em conjunto, estão dispostas e são operadas de forma a formarem um todo.

A área de aplicação da diretiva sobre máquinas estende-se assim desde uma máquina simples a uma instalação.

O cumprimento dos requisitos básicos de segurança e de saúde no anexo I da diretiva, é decisivo para a segurança das máquinas. O fabricante tem de respeitar os princípios de integração da segurança referidos no anexo I parágrafo 1.1.2.

Os objetivos de proteção têm de ser integrados de forma responsável, de forma a preencher a exigência em conformidade com a diretiva. O fabricante de uma máquina tem de apresentar o comprovativo da conformidade com os requisitos essenciais. Este comprovativo é facilitado mediante a aplicação de normas harmonizadas. Segundo o anexo IV da diretiva sobre máquinas, para as máquinas que apresentam um elevado potencial de risco é solicitado um procedimento de certificação. (Recomendação: Mesmo as máquinas que não são referidas no anexo IV, podem apresentar um grande potencial de risco e devem ser tratadas como tal.)

Esquema 4-1 Diretivas europeias para máquinas

## Normas

Para que os produtos possam ser comercializados ou operados, é necessário que preencham os requisitos básicos de segurança das diretivas UE. As normas podem ser muito úteis para o preenchimento destes requisitos de segurança. Além disso, na UE deve fazer-se a distinção entre normas que estão harmonizadas numa diretiva UE, e normas que estão ratificadas, mas não estão harmonizadas numa determinada diretiva, tais como outras regras técnicas, também referidas na diretiva como "normas nacionais".

As normas ratificadas descrevem o estado da tecnologia reconhecido. Ou seja, o fabricante pode comprovar que cumpriu com o estado da tecnologia reconhecido, aplicando-o.

Por princípio, todas as normas que estão ratificadas como normas europeias, têm de ser adotadas sem alterações no conjunto de normas dos estados-membros, independentemente de estarem harmonizadas numa diretiva, ou não. As normas nacionais existentes sobre o mesmo tema devem ser retiradas. Desta forma, pretende-se obter ao longo do tempo um conjunto de normas comuns (consistentes) na Europa.

### Normas europeias harmonizadas

As normas europeias harmonizadas (normas EN) são publicadas nos jornais oficiais da Comunidade Europeia e depois adotadas sem alterações nas normas nacionais.

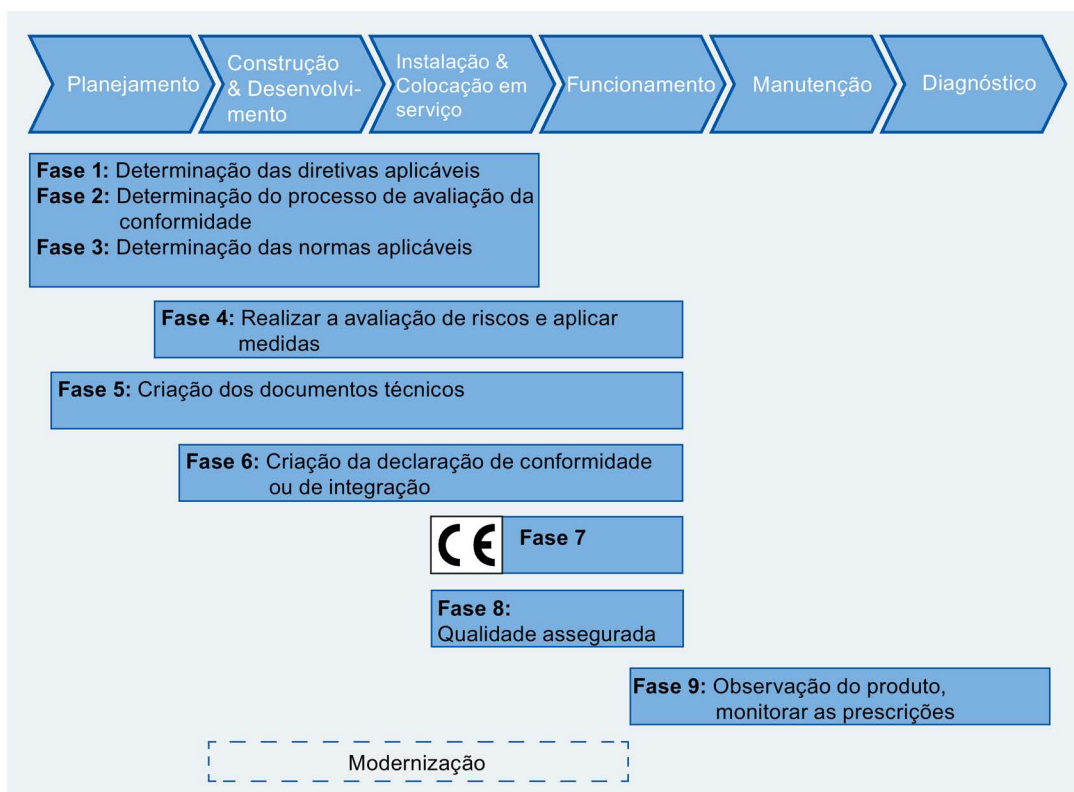
Estas servem para preencher os requisitos básicos de segurança e de saúde e os objetivos de proteção referidos no anexo I da diretiva sobre máquinas.

Através do cumprimento das normas harmonizadas resulta um "efeito automático de suposição" do preenchimento da diretiva, ou seja, o fabricante pode confiar que preencheu os aspetos de segurança da diretiva, desde que estes sejam abordados na respectiva norma. Contudo, nem todas as normas europeias estão harmonizadas neste sentido. Decisiva é a listagem no jornal oficial europeu. Estas listas estão sempre atualizadas e podem ser consultadas na internet (http://www.newapproach.org/).

## 4.1.1.2 Processo de conformidade CE

## Processo de conformidade CE

## Fases no processo de conformidade CE

O processo de conformidade CE divide-se em diferentes fases que têm de ser executadas durante todo o ciclo de vida (planejamento, construção, instalação, operação e manutenção).

Esquema 4-2 Processo de conformidade CE para máquinas e instalações

As diretivas aplicáveis devem ser definidas na fase 1, logo desde o planejamento. Isso pode abranger nenhuma, uma ou várias diretivas. (p. ex. diretiva sobre máquinas ver o capítulo 2.2.1)

Na fase 2 é definido o procedimento de avaliação da conformidade de acordo com as diretivas aplicáveis da fase 1.

Na fase 3 segue-se a determinação das normas aplicáveis.

A fase 4 subsequente é composta pela avaliação de riscos da máquina, pela redução de riscos e pela validação. A esta fase também pertence a avaliação das peças relativas à segurança do comando da máquina. Os passos individuais da fase 4 serão explicados nas secções seguintes.

A criação dos documentos técnicos é feita paralelamente a todo o planejamento, desenvolvimento e colocação em serviço, o que é designado como fase 5. Os documentos técnicos têm de estar completos quando a máquina é disponibilizada. Nestes incluem-se a documentação técnica (ver anexo VII da diretiva sobre máquinas), certificado de conformidade, se necessário, protocolos de recepção, documentos de transporte, etc.

Se a validação tiver sido efetuada com êxito, pode criar-se a declaração de conformidade e de integração na fase 6, e na fase 7 instalar-se a identificação CE na máquina.

Todos os fabricantes são obrigados a observar seus produtos após sua comercialização, no que respeita a eventuais deficiências escondidas. Isso é coberto pela qualidade assegurada da fase 8 e pela observação do produto da fase 9. Desta forma, devem recolher-se informações sobre se o produto é efetivamente utilizado como inicialmente previsto e sobre seu comportamento durante seu ciclo de vida.

Especialmente as deficiências no produto que possam originar perigos, tais como utilizações abusivas ou manuseamento incorreto, devem ser suprimidas mediante medidas adequadas. Se forem descobertas deficiências escondidas, será necessário informar o usuário.

## Avaliação de riscos

As máquinas e instalações implicam riscos devido à sua construção e funcionalidade. Por esse motivo, a diretiva sobre máquinas requer para cada máquina uma avaliação de riscos e, se necessário, uma redução de riscos, até que o risco residual seja menor do que o risco tolerável. Para o processo de avaliação destes riscos, deve utilizar-se a norma EN ISO 12100 "Segurança de máquinas - Princípios gerais de concepção - Avaliação e redução de riscos" (03 / 2011).

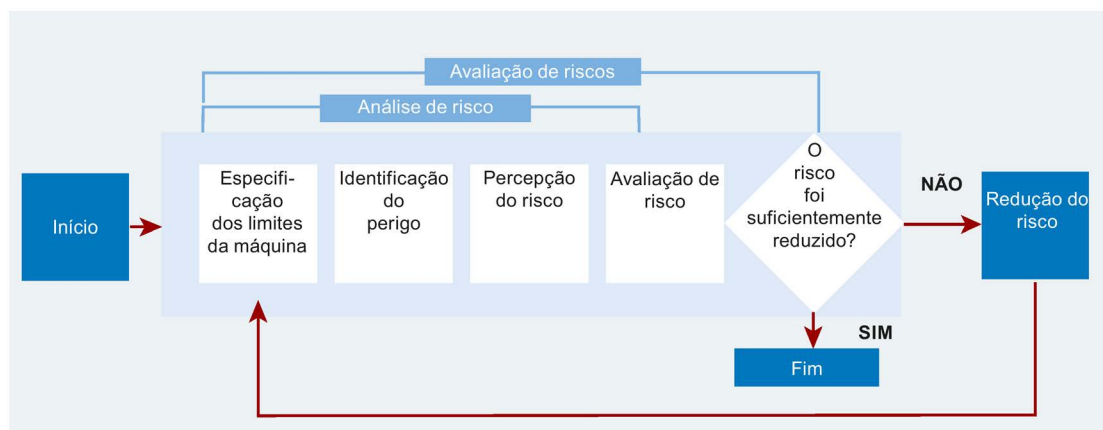
Concentrada em certos pontos principais, a norma EN ISO 12100 descreve os riscos a considerar, os princípios de concepção e o processo iterativo com avaliação e redução de riscos, para se alcançar a segurança.

A avaliação de riscos é uma sequência de passos que permite o controle sistemático de perigos provenientes de máquinas. Quando necessário, segue-se uma redução dos riscos após a avaliação de riscos. Da repetição deste procedimento resulta o processo iterativo, com a ajuda do qual os perigos podem ser eliminados, tanto quanto possível, e as medidas de proteção podem ser adotadas.

A avaliação de riscos abrange os seguintes passos:

- Análise de risco
  - Determinação dos limites da máquina
  - Identificação dos perigos
  - Percepção do risco
- Avaliação de risco

De acordo com o processo iterativo para se alcançar a segurança, realiza-se uma avaliação de risco após a percepção do mesmo. Aqui é necessário decidir se é necessário reduzir o risco. Se for necessário reduzir ainda mais o risco, deve se selecionar e aplicar medidas de proteção adequadas. A avaliação de riscos deve então ser repetida.

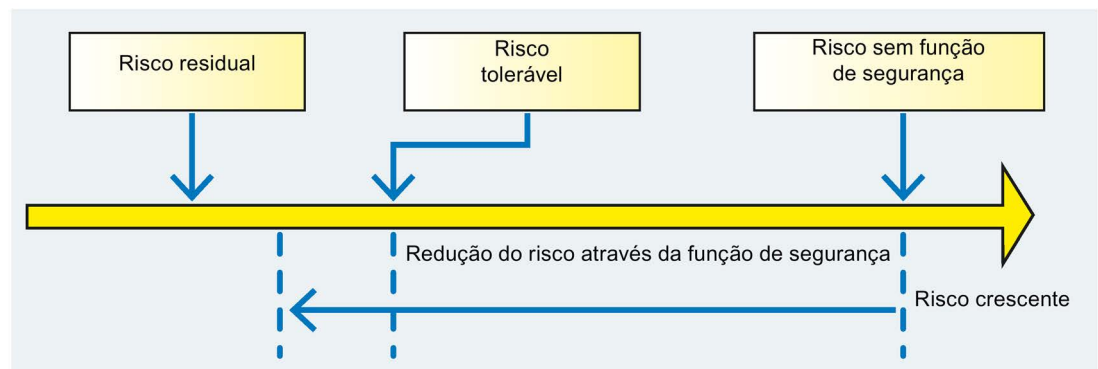
A redução dos riscos deve ser feita através da concepção e realização adequadas da máquina, p. ex. através do comando adequado ou medidas de proteção para as funções de segurança.

Esquema 4-3 Procedimento iterativo para a avaliação de riscos segundo EN ISO 12100

## Redução dos riscos

Se o risco estimado aparentar ser demasiado alto, terá de ser reduzido até que o risco residual seja menor do que o risco tolerável. Para o efeito, é necessário tentar primeiro tornar a máquina mais segura através de alterações na construção. Se isso não for possível, é necessário alcançar uma redução dos riscos através de medidas de proteção adequadas.

- A gravidade de um possível dano pode, p. ex., ser reduzida mediante a diminuição das velocidades dos movimentos ou forças de peças da máquina durante a ausência de pessoas.
- Através de dispositivos de fechamento é possível reduzir a frequência com que as pessoas permanecem na área de perigo.
- Existe sempre uma certa probabilidade de que uma máquina não se comporte como o previsto ou que instalações de proteção falhem. Tal pode ser causado por falhas em quaisquer peças da máquina. É possível alcançar uma redução do fator de risco através de uma construção adequada das peças relevantes à segurança. Às peças relevantes à segurança pertence também o comando da máquina, caso origine um perigo em caso de falha. O risco provocado pela falha do comando pode ser reduzido através de realização do comando segundo IEC 62061 ou ISO 13849-1.
- A possibilidade de evitar um dano pode ser aumentada, entre outros, através da detecção atempada de situações de perigo, p. ex., através de lâmpadas de sinalização.

Um parâmetro comum a todos estes elementos é a probabilidade de ocorrência de um evento indesejado. Reduzindo esta probabilidade é possível diminuir o risco.

Os seguintes passos devem ser executados para a redução dos riscos:

Esquema 4-4 Redução de riscos

### Passo 1: construção intrinsecamente segura

Uma construção intrinsecamente segura anula perigos ou reduz os riscos a eles inerentes através de uma seleção adequada de características construtivas da própria máquina e/ou através das interações entre as pessoas expostas aos perigos e a máquina.

Uma construção segura pode ser obtida, por exemplo, mediante a integração da segurança na máquina (coberturas, cercas, etc.). Estas medidas têm prioridade máxima no âmbito da redução de riscos. Deve-se:

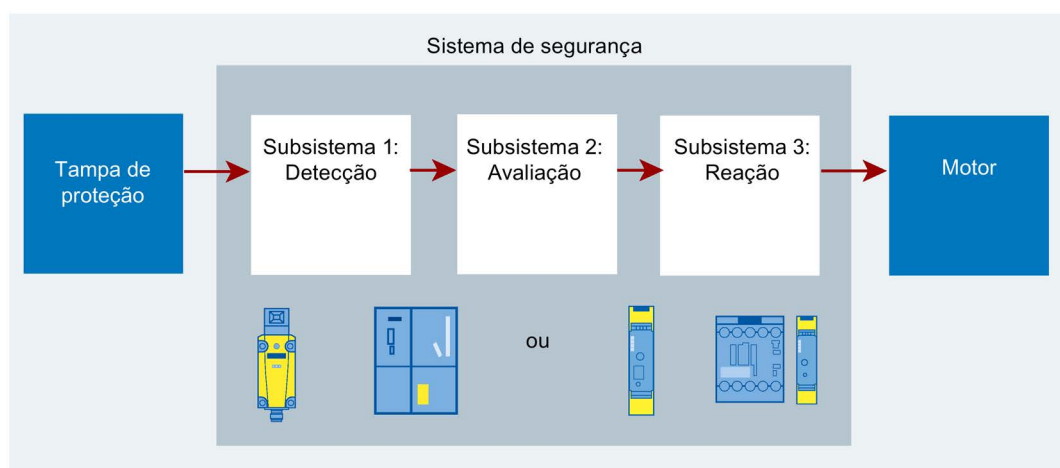
- Evitar locais de esmagamento
- Evitar choque elétrico
- Incluir conceitos para a paralisação em caso de emergência
- Incluir conceitos para a operação e manutenção

### Passo 2: medidas de proteção técnicas e/ou medidas de proteção complementares

Considerando a utilização para os fins previstos e a má utilização razoavelmente previsível, é possível aplicar medidas de proteção técnicas e complementares selecionadas de forma adequada, de forma a reduzir o risco, caso a eliminação de um perigo se revele impossível ou caso o risco a ele inerente não possa ser reduzido de forma satisfatória através de uma construção intrinsecamente segura.

O passo 2 inclui também todas as funções de comando relevantes à segurança de uma máquina. Para estas aplicam-se requisitos especiais cujo cumprimento tem de ser controlado.

Exemplo da estrutura de uma função de comando relevante à segurança:

- Detecção (interruptor de posição, parada de emergência, cortina de luz, etc.)
- Avaliação (comando com segurança contra falhas (failsafe), dispositivo de comutação de segurança, etc.)
- Reação (contator, conversor de frequência, etc.)

Esquema 4-5 Sistema de segurança para a função de segurança

### Passo 3: Informação para o usuário

Se, apesar da construção intrinsecamente segura e da utilização de medidas de proteção técnicas e complementares, ainda existirem riscos, é necessário que a informação para o usuário indique todos os riscos residuais.

Nestas informações para o usuário estão incluídas, por exemplo:

- Indicações de aviso nas instruções de funcionamento
- Instruções especiais de trabalho
- Pictogramas
- Indicações relativas à utilização de equipamento de proteção pessoal

Os requisitos para as peças relevantes à segurança dos comandos estão escalonados segundo o nível do risco ou a redução necessário do risco. A EN ISO 13849-1 utiliza o Performance Level (PL) escalonado hierarquicamente para a avaliação. A IEC 62061 utiliza a Safety Integrity Level (SIL) para o escalonamento. Ambas representam a medida para a capacidade de desempenho relevante em termos de segurança de uma função de comando.

Em todo o caso, é importante, independentemente de que norma é aplicada, que todas as peças do comando da máquina, que estão envolvidas na execução das funções relevantes à segurança, satisfaçam estes requisitos.

---

**Indicação**

Ao comando de uma máquina pertencem também os circuitos de corrente de carga das unidades propulsoras e motores.

---

Na concepção e realização do comando é necessário verificar se os requisitos do PL ou do SIL estão preenchidos. Como os requisitos para se alcançar o Safety Performance necessário estão estruturados de forma diferente em EN ISO 13849 e IEC 62061, também os requisitos para a verificação estão estruturados de forma diferente. Para um design segundo EN ISO 13849, estão descritos na Parte 2 (EN ISO13849-2) os pormenores para a validação e tudo o resto que tem de ser considerado. Os requisitos para a validação de um design segundo IEC 62061 estão descritos na própria norma.

## Validação

A validação significa uma verificação avaliadora da funcionalidade de segurança esperada. Sua finalidade é confirmar as determinações e o nível de conformidade das peças do comando relevantes à segurança dentro da determinação total para os requisitos de segurança da máquina. A validação também tem de demonstrar que todas as peças relativas à segurança preenchem os requisitos da norma relevante. Também são descritos os seguintes aspetos:

- Listas de falhas
- Validação das funções de segurança
- Validação do Safety Performance solicitado e do alcançado (categoria, Safety Integrity Level ou Performance level)
- Validação dos requisitos ambientais
- Validação dos requisitos de manutenção

Num plano de validação têm de ser descritos os requisitos para a execução da validação das funções de segurança definidas.

Objetivo da validação:

Determinação da conformidade com os requisitos

- das diretivas europeias.
- decorrentes da encomenda do cliente, da utilização da máquina e, se necessário, de outras exigências nacionais aplicáveis à máquina.

Todas as informações relevantes da máquina têm de ser apresentadas quando esta é disponibilizada. Nestas incluem-se: a encomenda do cliente, a documentação técnica (ver também o anexo VII da diretiva sobre máquinas), certificado de conformidade, se necessário, protocolos de recepção, documentos de transporte, etc.

## 4.2 Prescrições e normas fora da União Europeia (UE)

### 4.2.1 Prescrições e normas fora da União Europeia - Apresentação geral

A descrição seguinte deve fornecer uma visão geral das prescrições de alguns países fora da União Europeia. Esta não deve ser considerada como uma descrição completa. Os requisitos específicos, bem como as regras nacionais e locais para uma aplicação especial, devem ser controlados em detalhe para cada caso individual. Para mais informações relativas às especificações sobre engenharia de segurança em outros países, contate as respectivas entidades de homologação no local.

### 4.2.2 Requisitos legais nos EUA

Em relação aos requisitos legais sobre a segurança no local de trabalho, existe uma diferença significativa entre os EUA e a Europa, que consiste em que nos EUA não existe uma legislação federal comum sobre a segurança de máquinas que cubra a responsabilidade do fabricante/fornecedores. Cada vez mais se verifica o requisito geral de que o empregador tem de oferecer um local de trabalho seguro. Isso é regulado com a Occupational Safety and Health Act (OSHA) (ata sobre segurança e saúde ocupacional). As regras relevantes da OSHA para a segurança no trabalho estão descritas em OSHA 29 CFR 1910.xxx ("OSHA Regulations (29 CFR) PART 1910 Occupational Safety and Health"). (CFR: Code of Federal Regulations).

Paralelamente às regras da OSHA, é importante considerar as normas atuais de organizações como a NFPA e a ANSI bem como a responsabilidade global pelo produto existente nos EUA. Duas normas especialmente importantes para a segurança na indústria são NPFA 70 (conhecida como National Electric Code (NEC)) e NFPA 79 (Electrical Standard for industrial Machinery). Ambas descrevem os requisitos básicos das propriedades e execução de equipamento elétrico. A norma National Electric Code (NFPA70) é prioritária para edifícios mas também para as ligações elétricas de máquinas e quase-máquinas. A norma NFPA 79 aplica-se a máquinas. Daí advém uma zona cinzenta na delimitação entre as duas normas no caso de máquinas grandes, compostas por quase-máquinas. P. ex. os grandes sistemas de apoio podem ser considerados uma parte do edifício, pelo que terá de se utilizar a norma NFPA 70 e/ou NFPA 79.

### 4.2.3 Requisitos legais no Brasil

O Ministério do Trabalho e Emprego, órgão federal brasileiro responsável por regulamentar atividades no campo da saúde e segurança do trabalho publicou em Dezembro de 2010 a nova versão da Norma Regulamentadora No.12. Semelhante ao Artigo 137 das Diretivas Europeias, esta regulamentação se aplica tanto a máquinas novas como máquinas já existentes no parque instalado, e visa garantir a segurança na operação de máquinas por meio de recursos e tecnologias reconhecidamente eficazes. Baseada em Normas Internacionais, este regulamento brasileiro também considera o ciclo de vida total de uma máquina, desde a fase de projeto, passando pelas etapas de comercialização, transporte, chegando à operação e manutenção até a etapa final de descarte.

Embora a nova versão da NR 12 tenha sido baseada no modelo europeu, no qual a legislação (Diretivas) é suportada por normas internacionais, ela difere no que diz respeito aos instrumentos legais para avaliação da conformidade e uso de normas harmonizadas. Ao invés de validações feitas por entidades certificadoras, o próprio governo inspeciona máquinas e instalações, por meio de autoridades nominadas, no local da operação. Para tal, apenas os requerimentos específicos descritos na regulamentação são considerados. Por este motivo a NR 12 possui um conteúdo técnico adicional (Anexos) para máquinas específicas.

A NR 12 possui similaridade com as normas de segurança em termos estruturais. Ela possui requisitos gerais que podem ser satisfeitos por meio de uma Análise de Risco orientada por normas tipo A como a ISO12100, requisitos técnicos em conformidade com algumas normas tipo B e requisitos específicos para máquinas específicas, muito semelhantes às normas tipo C.

Os anexos da NR 12 não são harmonizados com normas tipo C, entretanto, a maioria deles foram elaborados com base em normas tipo C, ou de algum modo sofreram grande influência, de modo que pudessem alcançar os padrões ideais estabelecidos internacionalmente. Isto significa que embora a presunção de conformidade com a NR 12 não seja possível, mesmo assim, a maioria dos requerimentos da norma podem ser atendidos pela aplicação das normas tipo C.

Um breve resumo sobre a NR 12 será apresentado a seguir:

12.1 até 12.5: Princípios gerais e abrangência da norma.

12.6 até 12.13: Arranjo físico, instalações e condições ambientais no entorno das máquinas.

12.14 até 12.23: Instalações elétricas – aplicação de requisitos técnicos convencionais para instalações elétricas, painéis de comando e manobra (referências provenientes de EN 60204). Esta parte da NR 12 faz referência a outra norma regulamentadora relativa a instalações elétricas (NR 10).

**12.24 até 12.37: Sistemas de controle – aplicação de conceitos bem definidos na norma ISO 12100 relativos a comandos: disposição e tipos de comandos (bimanual em conformidade com EN 574), modos de seleção, prevenção contra partidas inesperadas, burla, uso de componentes adequados (mirror contacts) entre outros.**

**12.38 até 12.55: Sistemas de controle de segurança – requisitos gerais, comportamento em caso de falha, projeto orientado por categorias (NRB 14153 ou EN 954) alinhado à análise de riscos (ISO 12100). Esta parte também inclui requisitos para proteções fixas ou móveis intertravadas (EN 953, EN 1088).**

**12.56 até 12.63: Sistemas de parada de emergência – requisitos específicos (similar a ISO 13850).**

12.64 até 12.76: Meios de acesso permanentes a partes da máquina (posto de operação)

12.77 até 12.84: Sistemas pressurizados

12.85 até 12.93: Transportadores e equipamentos de elevação de cargas

12.94 até 12.105: Aspectos ergonômicos

12.106 até 12.110: Riscos adicionais

12.111 até 12.115: Manutenção, inspeção e ajuste de máquinas

12.116 até 12.124: Sinalização

12.125 até 12.129: Informações para uso, manuais, procedimentos

12.130 até 12.134: Procedimentos de segurança

12.135 até 12.147: Treinamento e capacitação

12.148 até 12.156: Requisitos complementares

**ANEXO I: Distâncias seguras para prevenir acesso a zonas perigosas (ISO 13852, ISO 13853, ISO 13854 e ISO 13855)**

ANEXO II: Treinamento

ANEXO III: Meios de acesso permanentes (EN 14122)

ANEXO IV: Termos e definições

ANEXO V: Motoserras

**ANEXO VI:** Máquinas para panificação e confeitaria

ANEXO VII: Máquinas para açougue e mercearia

**ANEXO VIII: Prensas mecânicas (EN 692), hidráulicas (EN 693) e similares**

**ANEXO IX: Máquinas injetoras de plástico (EN 201)**

ANEXO X: Máquinas para fabricação de calçados e afins

ANEXO XI: Máquinas e implementos para uso agrícola e florestal

NOTA: A NR 12 está atualmente sob revisão e novos anexos poderão ser inseridos posteriormente.

### 4.2.4 Requisitos legais na Austrália

A proteção da saúde no local de trabalho também desempenha um papel importante na Austrália.
Das diretivas revistas em janeiro de 2013 resultam novos requisitos também para as máquinas. Desta forma, as diretivas "Work Health and Safety Act 2012" e "Work Health and Safety Regulations 2012" desempenham um papel decisivo no contexto das respectivas regras de aplicação (Codes of Practice). Nas diretivas são definidas medidas para determinados perigos (como p. ex. cercas de proteção) de forma a assegurar um local de trabalho seguro. As regas de aplicação (Codes of Practice) contêm adicionalmente concretizações práticas e ajudas para a aplicação das diretivas, contudo, não são vinculativas.

# Especificação e design de comandos relevantes à segurança para máquinas 5

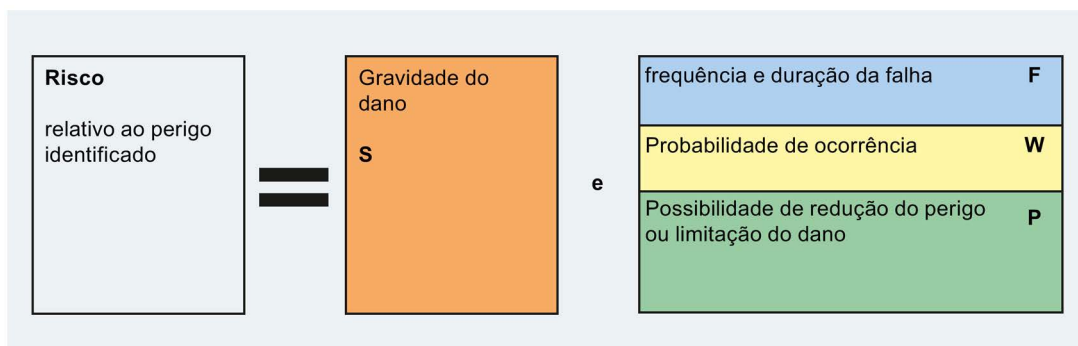
## 5.1 Peças relevantes à segurança para o comando da máquina

### 5.1.1 Quatro elementos de risco

#### Quatro elementos de risco

A avaliação de riscos permite a determinação do risco através de quatro elementos de risco:

- Gravidade do potencial dano
- Frequência com que as pessoas permanecem na área de perigo
- Probabilidade que o evento perigoso ocorra
- Possibilidade de evitar ou reduzir o dano

Estes elementos de risco, por sua vez, formam os parâmetros de entrada para a realização de uma função de comando relevante à segurança: Eles permitem, em primeiro lugar, a atribuição do risco aos requisitos do comando de segurança. Assim a IEC 62061 apresenta procedimentos para a avaliação dos elementos de risco e a classificação do Safety Performance.

Esquema 5-1 Risco relativo ao perigo identificado

## Apuramento do Safety Performance (Safety Integrity) necessário

Se durante a avaliação de riscos for determinado que os erros de funcionamento do comando ou a falha de instalações de proteção podem originar um risco excessivamente elevado, então a probabilidade de estes se verificarem tem de ser reduzida até que o risco residual seja tolerável. Ou seja, o comando tem de alcançar um "Safety Performance" suficiente.

Em IEC 62061 existe um procedimento que utiliza o escalonamento quantificado orientado para as probabilidades e, consequentemente, hierárquico, do Safety Performance. O resultado da análise de risco é então o Safety Integrity Level (SIL) para as funções de segurança afetadas.

Em ISO 13849-1 existe um escalonamento idêntico quantificado e, consequentemente, hierárquico do Safety Performance. A medida aí designada como Performance Level (PL) está correlacionada com os SILs da IEC 62061 através das probabilidades de falha atribuídas.

Mediante a aplicação das normas EN ISO 13849-1 e IEC 62061 os fabricantes de máquinas obtêm a conformidade com a nova diretiva sobre máquinas e, com esta, a capacidade de exportação e a segurança da responsabilidade. Estas introduziram, paralelamente a considerações qualitativas, também aspetos quantitativos. Do processo da avaliação de risco derivam medidas de proteção para a redução do risco, que são descritas através de funções de segurança. De seguida, a solução da função de segurança é verificada e avaliada por componentes de hardware e, se necessário, software, até que a integridade de segurança solicitada na avaliação de riscos seja alcançada.

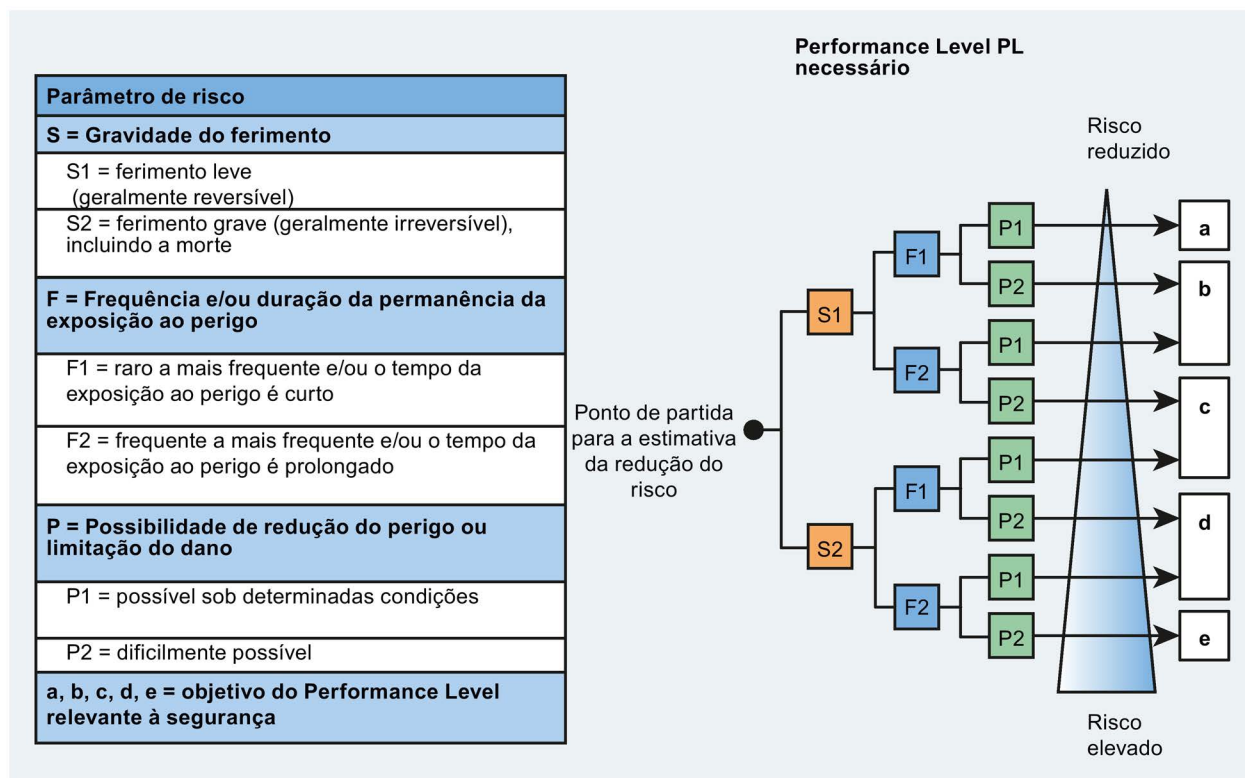
---

**Indicação**

Se existir uma norma C para o tipo de máquina considerado, devem-se realizar prioritariamente as medidas de proteção aí descritas. Contudo, é necessário controlar se as especificações estão atualizadas relativamente às mais recentes evoluções técnicas.

---

## Gráfico de risco segundo ISO 13849-1

O objetivo é determinar o Performance Level $PL_r$ solicitado, ou seja, a probabilidade de se verificarem falhas perigosas do sistema, através dos elementos de risco.

Esquema 5-2 Gráfico de risco segundo ISO 13849-1 para a determinação do Performance Level necessário

Para determinar o Performance Level necessário são utilizados os parâmetros **S** (gravidade do ferimento), **F** (Frequência/duração da exposição ao perigo) e **P** (possibilidade de evitação).

Relativamente à gravidade do ferimento (S) é feita a distinção entre reversível (p. ex. esmagamentos ou feridas) e irreversível (amputação, morte).

Para a frequência e duração da exposição ao perigo (F) não existem períodos de tempo universalmente válidos. Se uma pessoa for exposta ao perigo mais do que uma vez por hora (p. ex. para a colocação de peças) deve selecionar-se F2 (frequente a contínuo). Também é irrelevante se é a mesma pessoa ou se são diferentes pessoas que são expostas ao perigo. Se o acesso só tiver de ser feito esporadicamente, pode selecionar-se F1 (raro a menos frequente).

A possibilidade de evitação (P) é influenciada por vários aspetos. Aqui deve ser considerado o treinamento e o nível de conhecimentos do operador, bem como as possibilidades de evitação através de, p. ex., retirada e também operação com ou sem supervisão. O parâmetro **P1** (possível sob determinadas condições) só deve ser selecionado se existir efetivamente a possibilidade de evitar um acidente ou de reduzir consideravelmente a extensão de seus danos.

Os Performance Levels (PL) são uma medida quantitativa para o Safety Performance tal como o Safety Integrity Level (SIL) em IEC 61508 e IEC 62061.

### Safety Performance para a realização do comando segundo IEC 62061

O procedimento descrito em IEC 62061 no Anexo A utiliza um procedimento tabular, que pode ser utilizado diretamente para documentar a avaliação de risco e a atribuição SIL efetuadas.

Para os parâmetros individuais de risco deve selecionar-se a respectiva avaliação em função dos valores predefinidos no topo da tabela. Da soma dos pesos de todos os parâmetros resulta a classe da probabilidade do dano.

$K = F + W + P$

A frequência e a duração da permanência são expressas através do parâmetro "F". A necessidade de aceder à área de perigo pode divergir nos vários modos de funcionamento (funcionamento automático, funcionamento de manutenção, ...), também o tipo de acesso (ajustes das ferramentas, colocação de material,...) desempenha um papel e deve ser considerado sob este aspeto. A frequência e a duração em questão são selecionadas a partir da respectiva tabela. Se a duração da permanência for inferior a 10 minutos, o valor pode ser reduzido para o nível seguinte. Contudo, o valor para uma frequência ≤1 h nunca pode ser reduzido.

A probabilidade da ocorrência do evento perigoso é expressa através do parâmetro "W". Este tem de ser estimado independentemente dos outros parâmetros. Neste caso, também é necessário considerar o comportamento humano (condicionado por, p. ex., pressão do tempo, falta de consciência em relação ao perigo,...). Sob condições normais de produção e considerando o pior dos cenários, a probabilidade é "muito alta". Se for utilizado um valor baixo terá de existir uma justificação detalhada (p. ex. competências do operador de alto nível).

A possibilidade de evitar ou limitar o dano é expressa através do parâmetro "P". Aqui devem ser considerados aspetos que tanto dizem respeito à máquina (p. ex. a possibilidade de escapar ao perigo), como à possibilidade de detectar o perigo (p. ex. o alto ruído ambiente torna a detecção impossível). A classificação é feita de acordo com a tabela (provável, possível, impossível).

Com a ajuda da classe de probabilidade e da possível gravidade dos danos do perigo considerado, é possível consultar na tabela o SIL necessário para a respectiva função de segurança.

O objetivo é apurar o nível de integridade da segurança SIL do sistema através dos elementos de risco.

Esquema 5-3 Determinação do SIL necessário

# 5.2 Especificação dos requisitos de segurança

## Especificação dos requisitos de segurança

Se forem identificadas funções de segurança como relevantes à segurança ou se for necessário realizar medidas de proteção com meios do comando, os requisitos específicos para estas "funções de segurança" ("funções de comando relevantes à segurança") devem ser definidos na especificação dos requisitos de segurança ("safety requirements specification"). Esta especificação descreve para cada função relevante à segurança, entre outros:

- sua funcionalidade, ou seja, todas as informações de entrada necessárias, sua interligação e respectivos estados de saída ou ações, bem como a frequência de utilização
- os tempos de reação necessários
- o Safety Performance solicitado

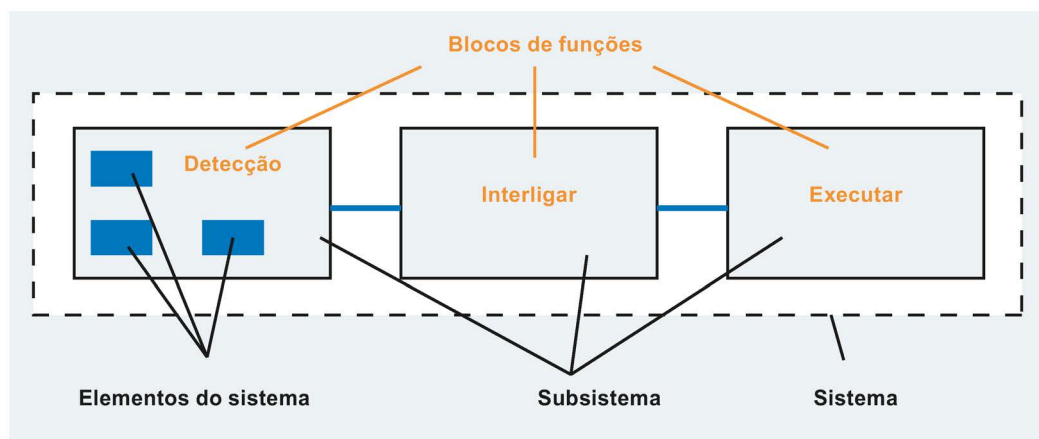
A especificação dos requisitos de segurança contém todas as informações necessárias à concepção e implementação do comando. Ela representa a interface entre o construtor da máquina e o fabricante/integrador do comando, podendo também servir para demarcar as responsabilidades.

# 5.3 Concepção e realização do comando (relevante à segurança) segundo IEC 62061

## 5.3.1 Filosofia/teoria

### Princípio de estruturação para um sistema de comando relevante à segurança

Um pré-requisito essencial para o funcionamento correto de um comando, e que esteja de acordo com as disposições, é sua construção correta. Para se alcançar este objetivo, a IEC 62061 definiu um processo de concepção descendente sistemático:

Um sistema elétrico de comando relevante em termos de segurança (Safety related electrical control system, SRECS) abrange todos os componentes, desde a recolha de informações, passando pela interligação das informações, até à execução de ações. Para possibilitar um procedimento sistemático na concepção, avaliação técnica de segurança e realização de um SRECS, que deva preencher os requisitos de IEC 61508, a IEC 62061 utiliza um princípio de estruturação que se baseia nos elementos de arquitetura seguintes (ver a figura seguinte).

Esquema 5-4 Elementos de estruturação da arquitetura do sistema

Em primeiro lugar, é feita a distinção entre uma "visão virtual (ou seja, funcional)" e a "visão real (ou seja, do sistema)". A visão funcional considera apenas os aspetos funcionais, independentemente da realização através do hardware e do software. Na visão virtual é considerado apenas, p. ex., que informações devem ser recolhidas, como estas devem ser interligadas e que ação deve resultar daí. Contudo, ainda não foram dados esclarecimentos sobre se, p. ex., são necessários sensores redundantes para a recolha de informações ou sobre como os atuadores serão realizados. Só com a "visão real" é que a realização através do SRECS é considerada. Aqui será então necessário decidir se, p. ex., para a realização da recolha de uma determinada informação serão necessários um ou dois sensores, para alcançar o Safety Performance solicitado. São definidos os seguintes termos.

### Termos para a estruturação das funções (visão funcional)

- **Bloco de funções**
  A unidade mais pequena de uma função de comando relevante à segurança (SRCF), cuja falha origina a falha da função de comando relevante à segurança.
  **Observação**: Em IEC 62061 um SRCF (F) é considerado como lógico "e" interligação dos blocos de funções (FB), p. ex. F = FB1 & FB2 & ... & FBn. A definição de um bloco de funções distingue-se da definição utilizada em IEC 61131 e em outras normas.
- **Elemento do bloco de funções**
  Parte de um bloco de funções.

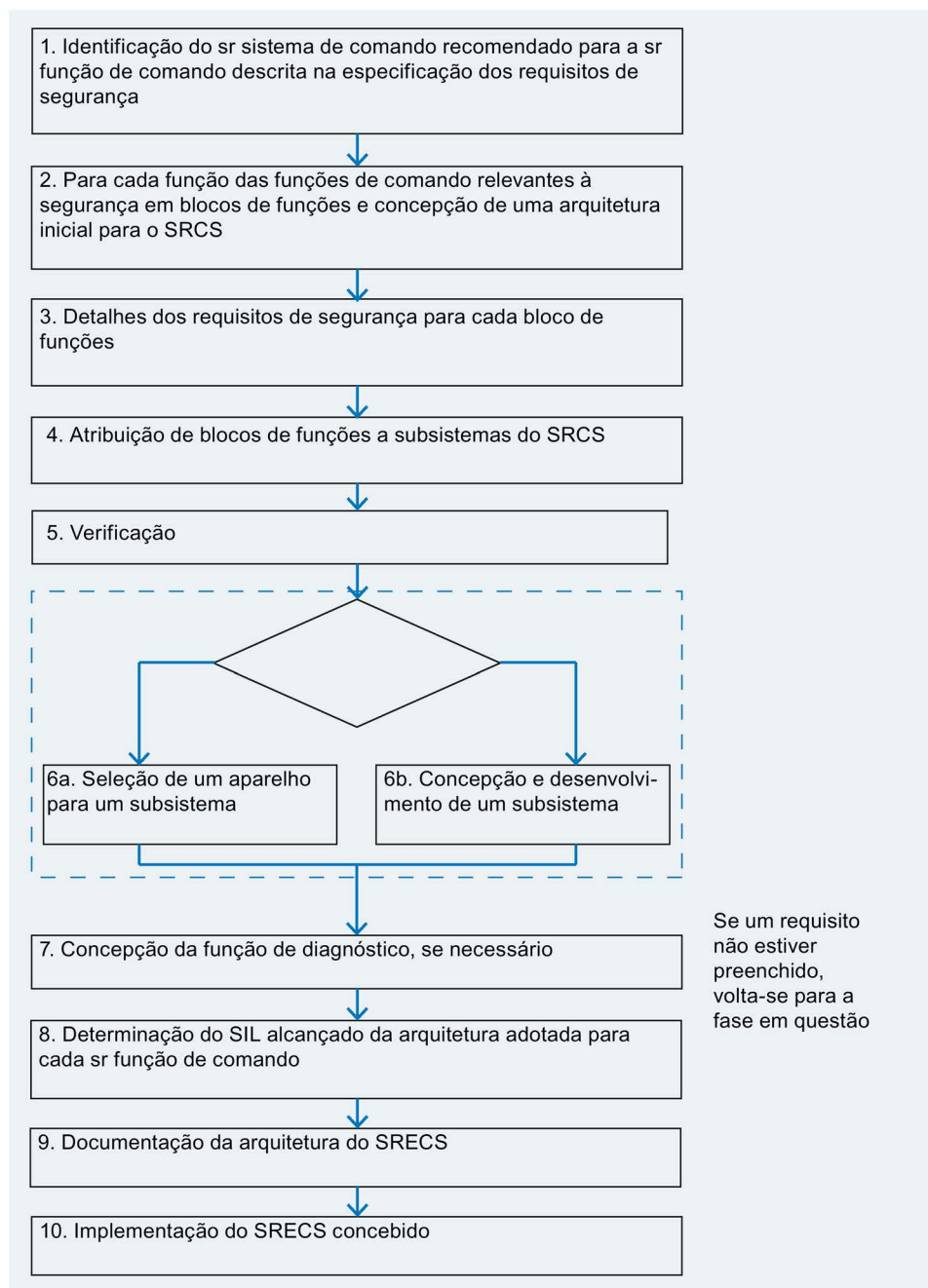
### Termos para a estruturação do sistema real (visão do sistema)

- **Sistema elétrico de comando relevante em termos de segurança**
  O sistema elétrico de comando de uma máquina, cuja falha pode originar um aumento imediato do risco.
  **Observação**: Um SRECS abrande todas as peças do sistema elétrico de comando, cuja falha pode originar uma redução ou perda da segurança funcional. Isso tanto pode abranger circuitos de energia como circuitos de comando.
- **Subsistema**
  Parte do design arquitetônico do SRECS ao mais alto nível, onde a falha de um subsistema qualquer origina a falha da função de comando relevante em termos de segurança.
  **Observação:** Contrariamente à linguagem corrente, na qual "subsistema" pode significar uma unidade subdividida qualquer, o termo "subsistema" é utilizado em IEC 62061 numa hierarquia de terminologia definida rigorosamente. "Subsistema" significa a subdivisão ao mais alto nível. As partes que provêm de uma outra subdivisão de um subsistema, são designadas como "elementos do subsistema"
- **Elemento do subsistema**
  Parte de um subsistema que abrange um único componente ou um grupo de componentes. Com estes elementos de estruturação é possível estruturar funções de comando segundo um procedimento claro, de forma que partes definidas da função (blocos de funções) de determinados componentes de hardware possam ser atribuídas aos subsistemas. Para os subsistemas individuais resultam assim requisitos claramente definidos, de forma a permitir a respectiva concepção e realização de forma independente uns dos outros. A arquitetura para a realização de todo o sistema de comando, resulta do fato de os subsistemas serem dispostos entre si tal como os blocos de funções estão dispostos dentro da função (lógica).

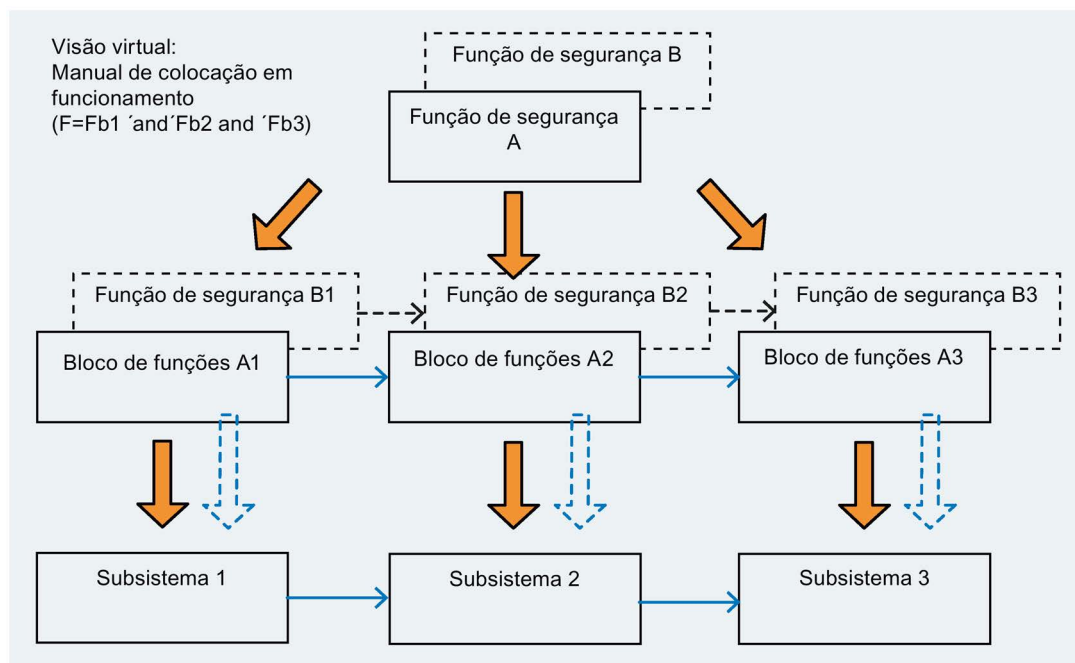
### 5.3.2 Processo de concepção de um sistema elétrico de comando relevante em termos de segurança SRECS

#### Processo de concepção

Se existir a especificação dos requisitos de segurança, o sistema de comando previsto pode ser concebido e implementado. Um sistema de comando, que preenche os requisitos específicos de uma determinada aplicação, não pode, de uma maneira geral, ser adquirido já pronto, terá sim de ser concebido e estruturado individualmente para a máquina em questão a partir de aparelhos disponíveis.

No processo de concepção, ocorre, em primeiro lugar, uma concepção gradual de uma arquitetura adequada do sistema de comando para cada função de segurança. De seguida, as arquiteturas de todas as funções de segurança da máquina em questão podem ser integradas num sistema de comando.

Esquema 5-5 Processo de concepção de um sistema de comando relevante à segurança

### Estruturação da função de segurança

O princípio básico da concepção estruturada consiste em subdividir cada função de comando em blocos de funções (pensados), de forma a permitir a atribuição de determinados subsistemas aos mesmos. A delimitação de cada bloco de funções é assim selecionada, de forma que estes possam ser inteiramente executados por determinados subsistemas. O importante nisto, é que cada bloco de funções representa uma unidade lógica, que tem de ser executada corretamente para que toda a função de segurança também o seja.

Esquema 5-6 Divisão de uma função de segurança em blocos de funções e atribuição aos subsistemas

### Safety Performance de um subsistema segundo IEC 62061

A "Safety Integrity" segundo IEC 62061 requer o preenchimento dos três requisitos básicos, que estão escalonados segundo o SIL:

1. Integridade sistemática,
2. Limitações estruturais, ou seja, tolerância de erros e
3. Probabilidade limitada de falhas acidentais perigosas (hardware) ($PFH_D$).

A integridade sistemática (1) de um sistema requerida para toda a função e as limitações estruturais (2), tanto se aplicam aos subsistemas individuais como ao sistema. Ou seja, quando um subsistema individual preenche a integridade sistemática requerida e as limitações estruturais de um determinado SIL, então preenche também o sistema. Contudo, se um subsistema preencher apenas os requisitos reduzidos de um SIL baixo, isso limita o SIL que o sistema pode alcançar. Assim, fala-se de "SIL claim limit" (SIL CL) de um subsistema.

- Integridade sistemática: SIL SYS <= SIL $CL_{lowest}$
- Limitações estruturais: SIL SYS <= SIL $CL_{lowest}$

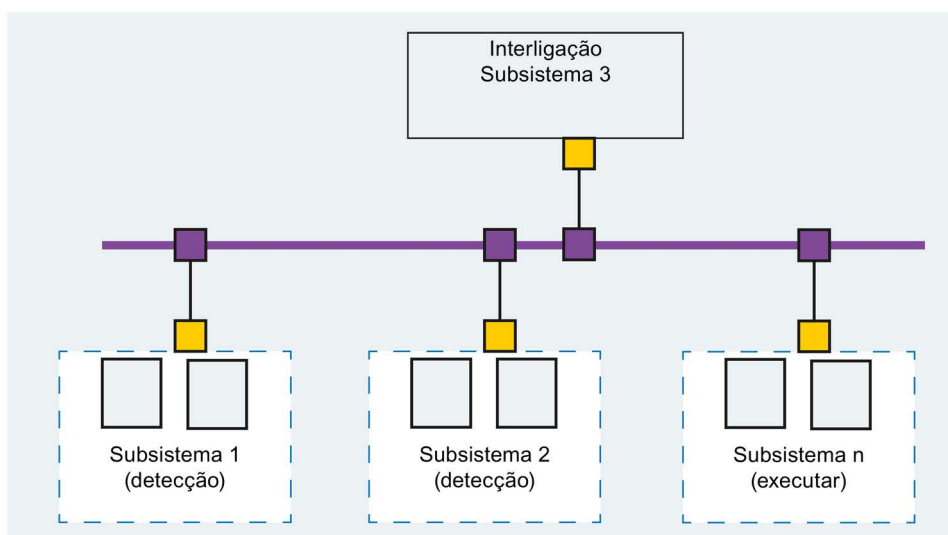
A limitação da probabilidade de ocorrerem erros acidentais perigosos (3) aplica-se para toda a função, ou seja, ela não pode ser ultrapassada por todos os subsistemas em conjunto. Assim, é válido:

$PFH_D = PFH_{D1} + ... + PFH_{Dn}$

### 5.3.3 Design do sistema para uma função de segurança

#### Concepção arquitetônica

A arquitetura de um sistema de comando para uma determinada função de segurança corresponde na sua estrutura lógica, à estrutura da função de segurança determinada anteriormente. Para se determinar a estrutura real do sistema, são atribuídos determinados subsistemas aos blocos de funções da função de segurança. Os subsistemas são então interligados, de forma a permitir o estabelecimento das ligações predefinidas através da estrutura da função. A conexão física é feita de acordo com as propriedades da tecnologia selecionada, p. ex., através de uma fiação individual (ponto para ponto) ou através de ligação bus.

Para outras funções de segurança da máquina ou instalação, o procedimento é o mesmo. Contudo, neste caso é possível atribuir blocos de funções, que correspondem a outras funções de segurança, aos mesmos subsistemas. Assim, quando é necessário, p. ex., recolher a mesma informação (p. ex. a posição da mesma porta de proteção) para duas funções diferentes, podem ser utilizados os mesmos sensores para o efeito.

Esquema 5-7 Exemplo de uma arquitetura do sistema para uma função de segurança

### Seleção de aparelhos adequados (subsistemas)

Um subsistema que deve ser utilizado para a implementação de uma função de segurança, tem de possuir a funcionalidade requerida e satisfazer os requisitos pertinentes da IEC 62061. Os subsistemas baseados em microprocessadores têm de preencher a IEC 61508 para o respectivo SIL.

Os subsistemas individuais têm de preencher os parâmetros de segurança exigidos na especificação (SIL CL e $PFH_D$).

Em muitos casos, os aparelhos necessitam ainda de medidas de detecção de erros adicionais (diagnóstico), de forma a alcançarem efetivamente o Safety Performance indicado para a sua utilização como subsistemas. Esta detecção de erros pode, p. ex., ocorrer através de aparelhos adicionais (p. ex. dispositivos de comutação de segurança SIRIUS 3SK1) ou de módulos de diagnóstico de software correspondentes no processamento lógico. Neste caso, a descrição do aparelho tem de conter as informações apropriadas.

Se não existir um aparelho adequado disponível, que preencha os requisitos de um subsistema com esta especificação, este terá de ser composto por aparelhos disponíveis. Isso requer um outro passo de concepção. Ver a este respeito a seção "Concepção e realização de subsistemas (Página 154)".

## 5.3.4 Realização do sistema de comando relevante à segurança

Um sistema de comando relevante à segurança tem de ser realizado de forma a preencher todos os requisitos de acordo com o SIL requerido. O objetivo é o de reduzir suficientemente a probabilidade de ocorrência de falhas sistemáticas ou acidentais, que possam originar uma falha perigosa da função de segurança. Devem ser considerados os seguintes aspetos:

- Integridade do hardware, ou seja, limitações arquitetônicas, (tolerância de erros) e probabilidade limitada de falha,
- Integridade sistemática, ou seja, requisitos para a evitação e controle dos erros,
- Comportamento no caso de detecção de um erro e design de software/desenvolvimento de software

## Integridade do hardware

Cada subsistema tem de ter uma tolerância de erros suficiente para o SIL do sistema. Esta depende de quão elevada é a percentagem de erros, que vão numa direção segura, relativamente à probabilidade de todos os erros possíveis do subsistema. Os erros potencialmente perigosos de um subsistema, que são descobertos atempadamente através do diagnóstico, pertencem aos erros que vão numa direção segura.

A probabilidade permitida de falha de uma função de segurança está limitada pelo SIL definido na especificação.

## Integridade sistemática

Devem ser aplicadas medidas para evitar erros sistemáticos bem como para controlar erros remanescentes no sistema.

**Evitação de erros sistemáticos:**

- O sistema deve ser instalado de acordo com o plano de segurança
- As informações fornecidas pelo fabricante do aparelho utilizado, devem ser seguidas
- Executar a instalação elétrica segundo IEC 60204-1 (7.2, 9.1.1 e 9.4.3)
- Verificar o design quanto à sua aptidão e correção
- Utilização de uma ferramenta informática, que utiliza elementos pré-configurados e testados.

**Controle dos erros sistemáticos:**

- Utilização do princípio de desligamento da energia
- Medidas para o controle de falhas ou interferências temporárias do subsistema, p. ex., devido a interrupções da tensão
- Se os subsistemas forem ligados através de um barramento, é necessário preencher os requisitos de IEC 61508-2 sobre a comunicação de dados (p. ex. PROFIsafe e ASIsafe)
- Os erros na ligação dos cabos (fiação) e nas interfaces dos subsistemas têm de ser detectados e têm de originar reações adequadas. Para o tratamento sistemático, as interfaces e a fiação são consideradas como parte integrante do subsistema em questão.

Para detalhes ver IEC 62061 6.4

### Comportamento no caso de detecção de um erro

Se os erros de um subsistema puderem originar uma falha perigosa de uma função de segurança, estes têm de ser descobertos atempadamente e tem de ocorrer uma reação adequada, para evitar o perigo. Em que medida é que a detecção automática de erros (diagnóstico) é necessária, depende das taxas de falha do aparelho utilizado e do SIL do sistema a alcançar (ou do PFH requerido do subsistema).

O modo como o sistema ou subsistema se deve comportar quando um erro é detectado, depende da tolerância de erros do subsistema em questão. Se o erro detectado não originar diretamente a falha da função de segurança, ou seja, tolerância de erros > 0, não é necessária uma reação imediata ao erro, a reação só é necessária quando a probabilidade para a ocorrência de um segundo erro se torna excessivamente elevada (geralmente são horas ou dias). Se o erro detectado originar diretamente a falha da função de segurança, ou seja, tolerância de erros = 0, é necessária uma reação imediata ao erro, ou seja, antes que se verifique um perigo.

#### 5.3.4.1 Safety Performance alcançado

## Safety Performance alcançado

Para cada função de segurança está definido na sua especificação, o Safety Performance de que ela necessita. Este tem de ser preenchido pelo sistema de comando relevante à segurança.

É necessário determinar para cada função de segurança, o Safety Performance que um sistema alcança. Isto é efetuado com base na arquitetura do sistema e dos parâmetros de segurança do subsistema que estão envolvidos na execução da função de segurança considerada.

### Design segundo IEC 62061

O SIL alcançado é limitado pela "aptidão SIL" dos seus subsistemas. O valor mais baixo do subsistema utilizado limita o SIL do sistema neste valor (o elo mais fraco de uma corrente determina a sua resistência.).

- Integridade sistemática: SIL SYS <= SIL $CL_{lowest}$
- Limitações estruturais: SIL SYS <= SIL $CL_{lowest}$

Para a interligação de subsistemas é necessário preencher os mesmos requisitos. Para o efeito, são consideradas fiações individuais como parte integrante de um dos dois subsistemas ligados. No caso de ligação bus, o hardware e o software emissor e receptor são parte integrante dos subsistemas.

Além desta aptidão fundamental, também é necessário considerar a probabilidade de ocorrência de uma falha perigosa em cada função de segurança. Esta valor resulta da simples adição das probabilidades de falha dos subsistemas envolvidos na função:

**$PFH_D = PFH_{D1} + ...+ PFH_{Dn}$**

No caso de ligações bus, é necessário adicionar ainda a probabilidade de possíveis erros na transmissão de dados (PTE).

O valor assim apurado para uma determinada função de segurança tem de ser menor (ou igual) do que o valor determinado pelo SIL correspondente.

Tabelas 5- 1 Valores limite das probabilidades de ocorrência de erros perigosos numa função de segurança

| Probabilidade de ocorrência de um erro perigoso por hora ($PFH_D$) | | | |
|---|---|---|---|
| | SIL 1 | SIL 2 | SIL3 |
| $PFH_D$ | $< 10^{-5}$ | $< 10^{-6}$ | $< 10^{-7}$ |

### 5.3.5 Integração do sistema para todas as funções de segurança

Depois de as arquiteturas de todas as funções de segurança terem sido concebidas, o passo seguinte é a integração destas arquiteturas específicas das funções no sistema de comando relevante à segurança completo.

Nos locais onde várias funções de segurança têm blocos de funções idênticos, podem ser utilizados subsistemas comuns para a sua realização:

- P. ex. quando se necessita de apenas um CLP de segurança para a implementação da lógica de todas as funções de segurança.
- Quando é necessário apurar o estado da mesma porta de proteção para a eliminação de diferentes perigos (ou seja, diferentes funções de segurança), o sensor necessário só tem de ser instalado uma vez nesta porta.

Isso não tem qualquer influência na Safety Integrity que já foi determinada para as funções individuais. Isso só tem de ser considerado nos aparelhos eletromecânicos (sujeitos a desgaste) quando é determinada a sua frequência de manobra.

### 5.3.6 Concepção e realização de subsistemas

Como alternativa à seleção de um subsistema existente, também é possível formar um subsistema a partir de aparelhos, que por si só não preenchem os requisitos de segurança, de forma que o subsistema alcance então o Safety Performance necessário. Isso diz respeito à integridade sistemática e às limitações estruturais provenientes do SIL claim limit (SIL CL) predefinido pelo SIL da função de segurança. Para a probabilidade de erros acidentais perigosos ($PFH_D$), foram definidos os valores PFH máximos para os subsistemas individuais, durante a concepção da arquitetura do sistema.

De uma forma geral, é necessária redundância pelo menos para SIL 2 e SIL 3. Quer seja para alcançar a tolerância de erros necessária, quer seja para permitir a detecção de erros (diagnóstico). A combinação de dois aparelhos num subsistema também pode ser necessária para reduzir a probabilidade de ocorrência de uma falha perigosa.

Os requisitos específicos para a concepção e realização de subsistemas estão descritos em IEC 62061 seções 6.7 e 6.8 . A descrição seguinte fornece uma visão geral.

## Concepção arquitetônica de um subsistema

É necessário conceber uma arquitetura especial do sistema, sempre que a Safety Integrity (Safety Performance) necessária não seja alcançada diretamente com os aparelhos previstos para uma determinada tarefa (subfunção, "bloco de funções"). De uma forma geral, as propriedades técnicas de segurança

- Probabilidade de falha reduzida
- Tolerância de erros, controle dos erros
- Detecção de erros

só podem ser alcançadas mediante medidas arquitetônicas especiais. Em que âmbito é que determinadas medidas são necessárias, depende do Safety Performance (Safety Integrity) requerido.

Ao subsistema está atribuído uma determinada (sub)função (p. ex., manter uma porta fechada), o bloco de funções. Este bloco de funções é primeiro (mentalmente) subdividido em elementos individuais (elementos do bloco de funções), que podem então ser atribuídos a determinados aparelhos, os elementos dos subsistemas. Geralmente é possível atribuir a mesma função a dois elementos do bloco de funções (a função foi praticamente duplicada). Se estes elementos do bloco de funções forem realizados através de aparelhos próprios, o subsistema tem uma tolerância de erros simples (redundância simples).

## Detecção de erros de um subsistema (diagnóstico)

Num subsistema sem tolerância de erros, cada erro origina a perda da função. A falha da função pode originar um estado perigoso ou seguro da máquina, em função do tipo de erro. Críticos são os erros que originam um estado perigoso da máquina. Estes são designados como "erros perigosos". Para evitar que um erro perigoso origine efetivamente um perigo, é possível detectar determinados erros através do diagnóstico e colocar a máquina num estado seguro antes que o perigo se verifique. Um erro perigoso detectado através do diagnóstico pode, assim, ser transformado num "erro seguro".

No caso de um subsistema redundante, o primeiro erro não origina logo a falha da sua função. Só um segundo erro é que pode originar a perda da função. Para evitar a falha do subsistema, é necessário detectar o primeiro erro antes que ocorra um segundo erro. A detecção de erros tem de estar naturalmente associada a uma reação adequada do sistema. No caso mais simples, p. ex., a máquina é parada para que seja colocada num estado seguro que não necessite da função de segurança (com erro).

Mediante a detecção de erros (diagnóstico) associada a uma reação adequada ao erro, é reduzida em ambos os casos a probabilidade de ocorrência de uma falha perigosa da função de segurança em questão. Em que medida é que a probabilidade é reduzida, depende, entre outros, da quantidade detectada de eventuais erros perigosos. A medida para tal é a cobertura de diagnóstico (diagnostic coverage DC).

A detecção de erros de um subsistema pode ser feita no próprio subsistema em questão ou através de um outro aparelho, p. ex., o CLP de segurança.

## Integridade sistemática de um subsistema

Para o design e implementação de um subsistema, é necessário adotar medidas tanto para evitar como para controlar erros sistemáticos, p. ex.:

- Os aparelhos utilizados têm de preencher as respectivas normas internacionais.
- As condições de utilização indicadas pelo fabricante têm de ser respeitadas.
- O design e os materiais utilizados têm de resistir a todas as condições ambientais previstas.
- O comportamento em função das influências ambientes tem de ser predeterminado, para que o estado seguro da máquina possa ser mantido.
- Detecção de erros On-line
- Ativação forçada para iniciação de uma medida de proteção

Os requisitos descritos em IEC 62061 referem-se unicamente ao design de subsistemas elétricos menos complexos, ou seja, não se referem aos subsistemas com microprocessadores. As medidas exigidas aplicam-se de mesma maneira a todos os SILs.

## Probabilidade de falha ($PFH_D$) de um subsistema

As eventuais falhas são distinguidas entre falhas "seguras" ou "perigosas". Desta forma, as falhas perigosas de um subsistema são definidas como segue.

## Falha perigosa

Falha de um SRECS, de um subsistema ou elemento de um subsistema com o potencial de originar um perigo ou um estado operacional.

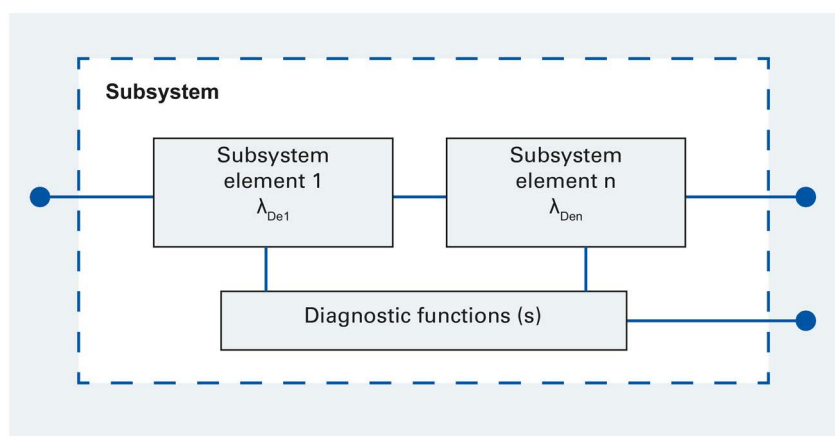
Observação: Se um estado destes se verifica ou não, pode depender da arquitetura do sistema; em sistemas com vários canais para uma melhoria da segurança, é pouco provável que uma falha perigosa do aparelho origine um estado geral perigoso ou uma falha de funcionamento.

Isso significa, p. ex.: No caso de um subsistema redundante (ou seja, tolerância de erros 1), o erro de um canal é designado como perigoso, quando é potencialmente perigoso, ou seja, que pode originar um estado perigoso da máquina caso não exista um segundo canal.

Para os requisitos de segurança só é determinante a probabilidade de ocorrência de falhas perigosas. Os chamados "erros seguros" pioram a disponibilidade do sistema mas não originam qualquer perigo.

A probabilidade de falha de um subsistema depende das taxas de falha do aparelho no qual o subsistema está montado, da arquitetura e das medidas de diagnóstico. As fórmulas para as duas arquiteturas mais usuais estão indicadas em IEC 62061.

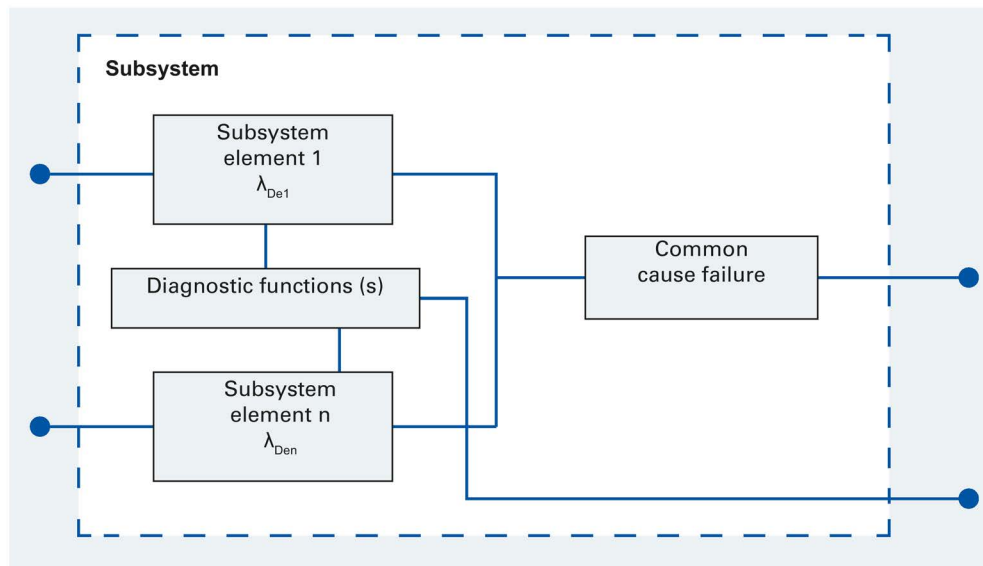
## Estrutura sem tolerância de erros com diagnóstico

No caso desta estrutura (ver a figura seguinte) o subsistema falha, quando qualquer um dos seus elementos falha, ou seja, um único erro origina a falha da própria função de segurança. Contudo, isso não significa obrigatoriamente uma perda perigosa da função de segurança. A máquina pode entrar num estado seguro ou perigoso em função do tipo de erro, ou seja, o subsistema tem um erro "seguro" ou "perigoso". Se a probabilidade de ocorrerem erros perigosos (PFHd) for maior do que o indicado na especificação, estes erros terão de ser detectados através do diagnóstico e terá de ocorrer uma reação ao erro antes que se verifique um perigo. Desta forma, os erros perigosos tornam-se em erros seguros e, consequentemente, a probabilidade de ocorrer uma falha perigosa do subsistema é reduzida, permitindo eventualmente que a probabilidade de falha permitida na especificação seja alcançada.

Esquema 5-8 Estrutura lógica de um subsistema sem tolerância de erros com diagnóstico

### Estrutura com tolerância de erros simples e com diagnóstico

No caso desta estrutura (ver a figura seguinte) o primeiro erro não origina logo a falha da função. Contudo, o erro tem de ser detectado antes que a probabilidade para a ocorrência de um segundo erro, ou seja, a falha do subsistema, ultrapasse o limite indicado na especificação.

Para além dos erros independentes e acidentais, deve-se ter ainda em conta nos subsistemas redundantes a possibilidade de erros com causa comum (common cause failure). A redundância homogênea não representa uma ajuda no caso destes erros. Assim, é necessário adotar medidas sistemáticas durante a concepção que tornem sua probabilidade suficientemente baixa. Devido à impossibilidade de excluir totalmente os erros com causa comum, estes devem ser considerados durante o cálculo da probabilidade de falha do subsistema. Isso é feito com a ajuda do fator de causa comum (β), com o qual é avaliada a eficácia das medidas adotadas. No anexo F de IEC 62061 encontra-se uma tabela para a determinação do fator de causa comum alcançado.

No caso desta estrutura, uma falha isolada de um elemento do subsistema não origina a falha de função de comando relevante à segurança.

Esquema 5-9 Estrutura lógica de um subsistema com tolerância de erros simples com diagnóstico

## Limitações estruturais de um subsistema

As limitações estruturais requerem um mínimo de tolerância de erros em função do tipo do possível erro do subsistema. Quanto maior for a percentagem de erros "seguros", menor é a tolerância de erros requerida para um determinado SIL.

A tabela seguinte mostra os respectivos limites. Neste contexto, os "erros seguros" também são os erros potencialmente perigosos detectados através do diagnóstico.

Tabelas 5- 2 Limitações estruturais de um subsistema

| Percentagem de erros seguros | Tolerância de erros de hardware | |
|---|---|---|
| | 0 | 1 |
| < 60 % | Não permitido<br>(ver a norma para as exceções) | SIL 1 |
| 60 % até < 90 % | SIL 1 | SIL 2 |
| 90 % até < 99 % | SIL 2 | SIL 3 |
| ≥ 99 % | SIL 3 | SIL 3 |
| Observação: Uma tolerância de erros de hardware de N significa que erros N+1 podem originar a perda da função. | | |

Assim, p. ex., não é requerida qualquer tolerância de erros (FT = 0) para um subsistema que deve ser utilizado para SIL 2, se a percentagem dos seus erros , que vão numa direção segura, for superior a 90 %. A maioria dos aparelhos não consegue alcançar este valor por eles mesmos. Contudo, é possível reduzir a percentagem de erros perigosos, mediante a detecção dos erros através do diagnóstico e a execução atempada de uma reação adequada.

A safe failure fraction de um subsistema é a percentagem de erros que originam um estado seguro da máquina, ponderada com base na quantidade total de erros do subsistema segundo a sua probabilidade de ocorrência.

## 5.4 Concepção e realização das partes relevantes em termos de segurança de um comando segundo ISO 13849-1

### Objetivo

Um sistema (de comando) relevante à segurança tem de executar corretamente uma função de segurança. Mesmo em caso de falha, este tem de se comportar de forma que a máquina ou instalação permaneça ou seja colocada num estado seguro.

### Apuramento do Safety Performance (Safety Integrity) necessário

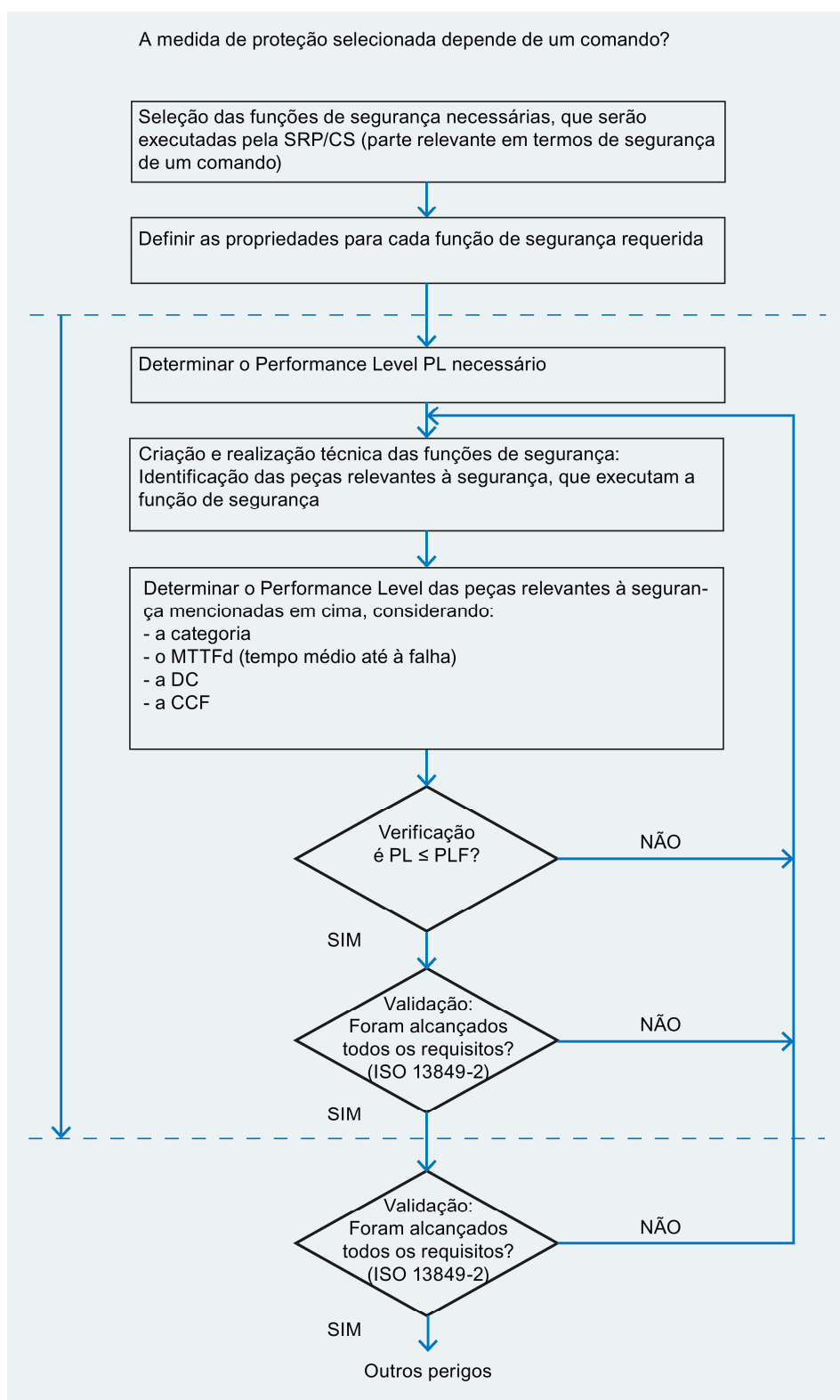
Os requisitos da função de segurança foram determinados através do processo da avaliação de riscos (ver o capítulo "Peças relevantes à segurança para o comando da máquina (Página 137)").

A ISO 13849-1 prescreve o Performance Level $PL_r$ necessário. Ver a este respeito o capítulo "Peças relevantes à segurança para o comando da máquina (Página 137)".

### Processo de concepção das partes relevantes em termos de segurança de um comando

As categorias segundo ISO 13849-1 tanto dizem respeito ao sistema (função de segurança) como a seus subsistemas. Na realização segundo ISO 13849-1 é possível utilizar o mesmo princípio de estruturação do sistema relevante à segurança que o descrito em IEC 62061. Cada subsistema assim delimitado tem de alcançar o Performance Level solicitado para a função de proteção. Os requisitos da categoria em questão também se aplicam para a fiação de subsistemas entre si.

Para a concepção e paralelamente às categorias, na ISO 13849-1 é introduzido adicionalmente o Performance Level $PL_r$ como a grandeza quantitativa para a probabilidade de falha.

A figura seguinte mostra o processo iterativo para a criação das peças de comandos (SRP / CS) relevantes à segurança:

Esquema 5-10 Processo iterativo para a criação das peças de comandos relevantes à segurança

## Concepção segundo ISO 13849-1

A concepção arquitetônica orienta-se pelo Performance Level $PL_r$ necessário.

O conceito de concepção de ISO 13849-1 baseia-se em arquiteturas especiais predefinidas das peças do comando relevantes à segurança.

Uma função de segurança pode ser composta por uma ou várias peças de um comando (SRP / CS) relevantes à segurança.

Uma função de segurança também pode ser uma função operacional, como p. ex., um comando bimanual para a iniciação de um processo.

Uma função de segurança típica é composta pelas seguintes peças de um comando relevantes à segurança:

- Entrada ($SRP/CS_a$)
- Lógica/processamento ($SRP/CS_b$)
- Saída/elemento de transmissão de energia ($SRP/CS_c$)
- Ligações ($i_{ab}$, $i_{ac}$) (p. ex. elétricas, ópticas)

Observação: As peças relevantes à segurança são compostas por um ou mais componentes; os componentes podem ser compostos por um ou mais elementos.

Todos os elementos de ligação estão incluídos nas peças relevantes à segurança.

Uma vez determinadas as funções de segurança do comando, é necessário identificar as peças do comando relevantes à segurança. É igualmente necessário avaliar o seu contributo para o processo de redução de riscos (ISO 12100).

## Performance Level PL

Na aplicação da ISO 13849, a capacidade de peças relevantes à segurança realizarem uma função de segurança é expressa pela determinação de um Performance Level.

Para cada SRP/CS (parte relevante em termos de segurança de um comando) selecionado e/ou combinação de SRP/CS, que executa uma função de segurança, é necessário fazer uma estimativa do PL.

O PL de SRP/CS tem de ser determinado através da estimativa dos seguintes aspetos:

- $MTTF_d$ (tempo médio até ocorrer a falha perigosa)
- DC (cobertura de diagnóstico)
- CCF (falha devido a causas comuns)
- Estrutura
- Comportamento da função de segurança sob condição(ões) de erro
- Software relevante em termos de segurança
- Falhas sistemáticas

### Tempo médio até ocorrer a falha perigosa de cada canal ($MTTF_d$)

O valor de $MTTF_d$ de cada canal é indicado em três níveis e tem de ser considerado individualmente para cada canal (p. ex. canal individual ou cada canal de um sistema redundante). Em relação ao $MTTF_d$ é possível definir um valor máximo de 100 anos.

| $MTTF_d$ | |
|---|---|
| Baixo | 3 anos ≤ $MTTF_d$ < 10 anos |
| Médio | 10 anos ≤ $MTTF_d$ < 30 anos |
| Alto | 30 anos ≤ $MTTF_d$ ≤ 100 anos |

### Cobertura de diagnóstico (DC)

O valor para DC é indicado em quatro níveis. Para se estimar a DC é possível, na maioria dos casos, utilizar a análise de potenciais falhas e influências (FMEA) ou processos idênticos. Neste caso, é necessário considerar todas as falhas relevantes e/ou tipos de falhas, e controlar o PL da combinação de SRP/CS, que deve executar a função de segurança, relativamente ao Performance Level ($PL_r$ ) necessário. Para uma abordagem simplificada da estimativa de DC, ver ISO 13849-1 Anexo E.

| Cobertura de diagnóstico (DC) | |
|---|---|
| Nenhuma | DC < 60 % |
| Baixa | 60 % ≤ DC < 90 % |
| Média | 90 % ≤ DC < 99 % |
| Alta | 99 % ≤ DC |

## 5.4.1 Concepção e realização de categorias

### Categoria B

Para se alcançar uma categoria B é necessário que as peças do comando relevantes à segurança cumpram os seguintes requisitos e sejam estruturadas, selecionadas e combinadas segundo os mesmos.

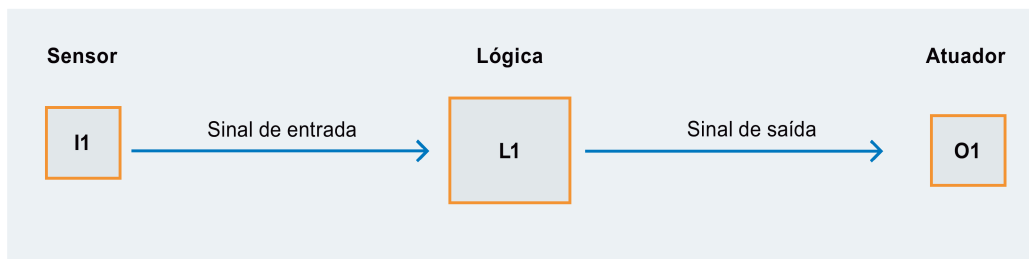
- Aplicação dos princípios básicos de segurança
- Resistência às solicitações de serviço previstas, a estas pertence a capacidade de comutação ou a frequência de manobra dos componentes
- Robustez relativamente às influências do material processado e condições ambientais, a estas pertencem p. ex., aparecimento de substâncias como óleos, produto de limpeza, nevoeiro salino
- Robustez relativamente a outras influências externas relevantes, a estas pertencem vibrações mecânicas, interferências eletromagnéticas, interrupção ou falha do fornecimento de energia.

Num sistema de categoria B o $MTTF_d$ de cada canal pode ser baixo a médio. Não existe uma cobertura de diagnóstico (DC avg = nenhuma). Como a estrutura geralmente é de um canal, a CCF não é considerada nesta categoria, por não ser relevante. O Performance Level máximo alcançável de um sistema da categoria B é PL = b.
Devido à estrutura de um canal, um erro pode originar a perda da função de segurança.

**Exemplo de uma arquitetura prevista da categoria B:**

- I1: Sensor 1 (p. ex. um interruptor de posição)
- L1: Unidade lógica 1 (p. ex. um dispositivo de comutação de segurança)
- O1: Atuador 1 (p. ex. um contator)

As propriedades estruturais são:

- Estrutura de um canal

Esquema 5-11 Arquitetura prevista para a categoria B

## Categoria 1

Para se alcançar uma categoria 1 é necessário que os requisitos estejam preenchidos, tal como para a categoria B.
Adicionalmente ainda é necessário implementar os seguintes requisitos:

Para as peças do comando relevantes à segurança é necessário utilizar componentes comprovados e respeitar princípios de segurança comprovados (ver ISO 13849-2).

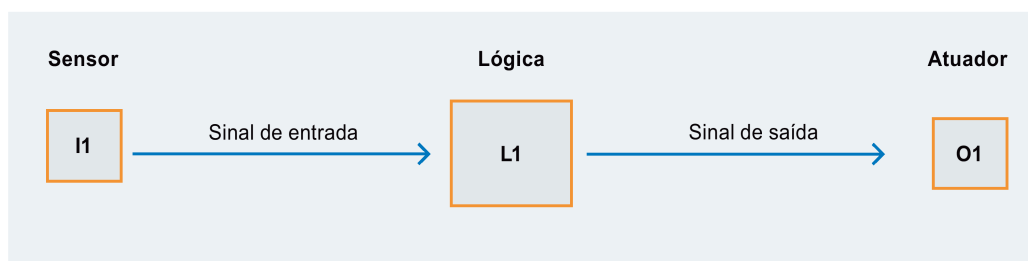
Num sistema de categoria 1 o MTTFd de cada canal tem de ser alto.

O Performance Level máximo alcançável é PL = c.

**Exemplo de uma arquitetura prevista da categoria 1:**

- I1: Sensor 1 (p. ex. um interruptor de posição)
- L1: Unidade lógica 1 (p. ex. um dispositivo de comutação de segurança)
- O1: Atuador 1 (p. ex. um contator)

As propriedades estruturais são:

- Estrutura de um canal
- Utilização de componentes comprovados

Esquema 5-12 Arquitetura prevista para a categoria 1

## Categoria 2

Para se alcançar uma categoria 2 é necessário que os requisitos estejam preenchidos, tal como para a categoria B. É igualmente necessário respeitar os princípios de segurança comprovados. Adicionalmente aplicam-se os seguintes requisitos:

As peças do comando relevantes à segurança de um sistema de categoria 2, têm de ser testadas em intervalos de tempo apropriados pelo comando da máquina. Este teste da função de segurança pelo comando da máquina tem de ser efetuado:

- No arranque da máquinas, bem como
- Antes do início de uma situação perigosa, p. ex., no início de um novo ciclo da máquina, iniciação de outros movimentos, etc.

Como resultado do teste efetuado pelo dispositivo de teste

- tem de ocorrer uma reação adequada ao erro sempre que é detectado um erro
- não pode ser autorizado o funcionamento se não for detectado qualquer erro

A reação ao erro tem de originar, sempre que possível, um estado seguro. Só quando o erro for eliminado é que o funcionamento normal pode prosseguir. Se não for possível alcançar o estado seguro (p. ex. no caso de contatos soldados), tem de ocorrer um aviso sobre o perigo.

Num sistema de categoria 2 o MTTFd de cada canal tem de ser baixo a alto, em função do PLr necessário. As peças do sistema de comando relevantes à segurança têm de apresentar uma cobertura de diagnóstico baixa a média. Ao mesmo tempo, têm de ser aplicadas medidas CCF (ver ISO 13849-1 Anexo F).

Adicionalmente, o próprio teste não pode originar outros perigos. O dispositivo de teste pode ser uma parte integrante das peças do sistema de comando relevantes à segurança ou também pode ser utilizado separado destas.

O Performance Level máximo alcançável de um sistema de categoria 2 é PL = d.

---

**Indicação**

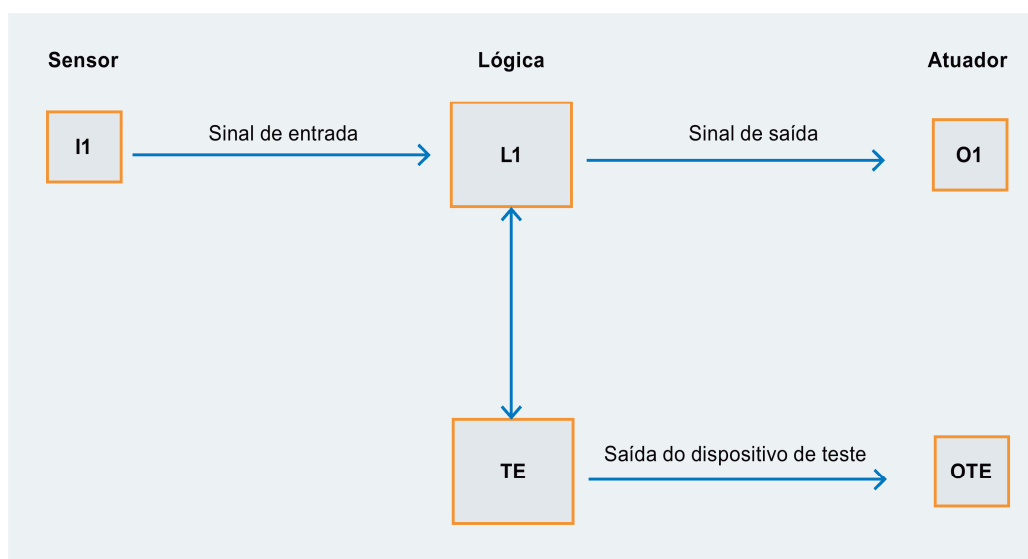
De acordo com o processo simplificado de ISO 13849-1, a categoria 2 representa um sistema testado de um canal: quando ocorre um erro perigoso, a detecção de erros só é eficaz (útil), quando o teste de detecção de erros ocorre antes do próximo requisito da função de segurança. Com base nisto, é solicitada uma taxa de teste 100 vezes maior do que a taxa de exigência da função de segurança.

---

**Exemplo de uma arquitetura prevista da categoria 2**

- I1: Sensor 1 (p. ex. um interruptor de posição)
- L1: Unidade lógica 1 (p. ex. um dispositivo de comutação de segurança)
- O1: Atuador 1 (p. ex. um contator)
- TE: Dispositivo de teste

As propriedades estruturais são:

- Estrutura de um canal
- Monitoramento através do dispositivo de teste

Esquema 5-13 Arquitetura prevista para a categoria 2

## Categoria 3

Para se alcançar uma categoria 3 é necessário que os requisitos estejam preenchidos, tal como para a categoria B. É igualmente necessário respeitar os princípios de segurança comprovados. Adicionalmente aplicam-se os seguintes requisitos:

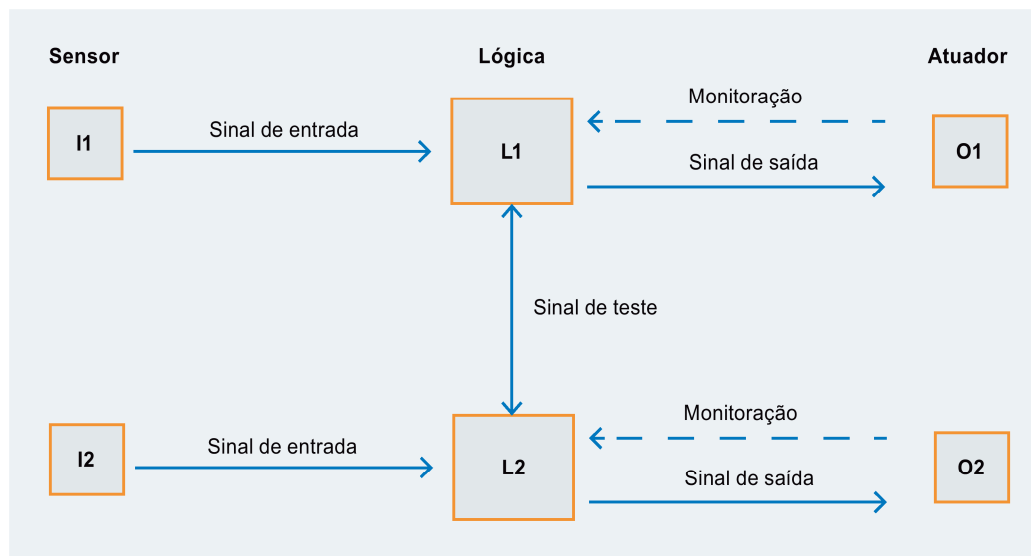
As peças do sistema de comando relevantes à segurança da categoria 3 têm de ser concebidas de forma que a ocorrência de um erro individual não origine a perda da função de segurança. Sempre que possível, o erro individual tem de ser detectado durante ou antes do próximo requisito da função de segurança.

Num sistema de categoria 3 o MTTFd de cada canal redundante tem de ser baixo a alto, em função do PLr necessário. As peças do sistema de comando relevantes à segurança têm de apresentar uma cobertura de diagnóstico baixa a média. Ao mesmo tempo, têm de ser aplicadas medidas CCF (ver ISO 13849-1 Anexo F).

### Exemplo de uma arquitetura prevista da categoria 3:

- I1 e I2: Sensores 1 e 2 (p. ex. dois interruptores de posição com contatos de abertura positiva)
- L1 e L2: Unidades lógicas 1 e 2 (um dispositivo de comutação de segurança, p. ex. já contém estas duas unidades)
- O1 e O2: Atuadores 1 e 2 (p. ex. dois contatores)

As propriedades estruturais são:

- Montagem redundante
- Monitoramento dos sensores (monitoramento da discrepância)
- Monitoramento dos circuitos de liberação (monitoramento, comparável com os circuitos de retorno atuais)

Esquema 5-14 Arquitetura prevista para a categoria 3

## Categoria 4

Para se alcançar uma categoria 4 é necessário que os requisitos estejam preenchidos, tal como para a categoria B. É igualmente necessário respeitar os princípios de segurança comprovados. Adicionalmente aplicam-se os seguintes requisitos:

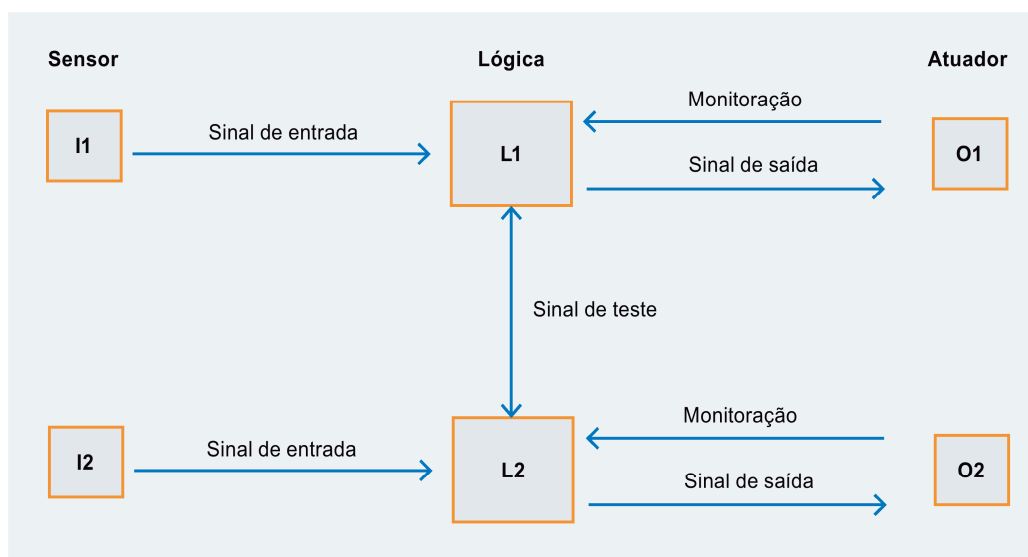
As peças do sistema de comando relevantes à segurança da categoria 4 têm de ser concebidas de forma que a ocorrência de um erro individual não origine a perda da função de segurança. O erro individual tem de ser detectado durante ou antes do próximo requisito da função de segurança. Se um erro não for detectado, a acumulação deste erro não pode originar a perda da função de segurança.

Num sistema de categoria 3 o MTTFd de cada canal redundante tem de ser alto. As peças do sistema de comando relevantes à segurança têm de apresentar uma cobertura de diagnóstico alta. Ao mesmo tempo, têm de ser aplicadas medidas CCF (ver ISO 13849-1 Anexo F).

Exemplo de uma arquitetura prevista da categoria 4:

- I1 e I2: Sensores 1 e 2 (p. ex. dois interruptores de posição com contatos de abertura positiva)
- L1 e L2: Unidades lógicas 1 e 2 (um dispositivo de comutação de segurança, p. ex. já contém estas duas unidades)
- O1 e O2: Atuadores 1 e 2 (p. ex. dois contatores)

As propriedades estruturais são:

- Montagem redundante
- Monitoramento dos sensores (monitoramento da discrepância)
- Monitoramento dos circuitos de liberação (monitoramento, comparável com os circuitos de retorno)
- Elevada cobertura de diagnóstico em todos os subsistemas

Esquema 5-15 Arquitetura prevista para a categoria 4

## Avaliação das funções de segurança

Cada função de segurança prevista, bem como sua implementação e avaliação, tem de ser documentada de acordo com as especificações da norma.

Para a avaliação de funções de segurança nas máquinas e instalações, o manuseamento rápido e simples da Safety Evaluation Tool da SIEMENS oferece-lhe um suporte valioso.

A Tool On-line aprovada pelo TÜV orienta o usuário passo a passo desde a determinação da estrutura do sistema de segurança, passando pela seleção dos componentes, até à seleção dos componentes para a determinação da integridade de segurança alcançada segundo ISO 13849-1 e IEC 62061.

Neste caso, as extensas bibliotecas integradas também lhe fornecem suporte. Como resultado, o usuário recebe um relatório conforme as normas, que pode ser integrado na documentação como comprovativo de segurança.

Através do acesso On-line da Safety Evaluation Tool é assegurado que os cálculos são sempre efetuados com as normas atuais e que se acessa sempre aos dados técnicos atuais de todos os componentes relevantes à segurança da SIEMENS.

A Safety Evaluation Tool está disponível na Internet (http://www.siemens.com/safety-evaluation-tool).

# 6 Assistência técnica e suporte

## 6.1 Assistência técnica e suporte

### Safety Integrated na Internet

Nossa presença On-line disponibiliza-lhe informações atuais sobre a engenharia de segurança. Aí encontra documentos úteis, links, filmes e ferramentas sobre produtos e soluções Safety Integrated, bem como sobre a aplicação das normas.
Safety Integrated na Internet (http://www.siemens.com/safety-integrated)

### Functional Safety Services

Nós fornecemos suporte, por exemplo, na realização da avaliação de riscos. Ou assumimos a verificação SIL ou PL de seu conceito, a programação da função de segurança ou a verificação da engenharia.

Functional Safety Services na Internet (http://www.siemens.com/safety-services)

### SITRAIN Treinamento para Safety Integrated

Avaliação de riscos, normas, identificação CE, treinamento para os produtos: Na Internet encontra todas as informações úteis sobre nosso programa de treinamento abrangente SITRAIN.

SITRAIN Treinamento para Safety Integrated na Internet (http://www.siemens.com/sitrain-safetyintegrated)

### Catálogos e material informativo

No centro de informação e download encontra todos os catálogos atuais, revistas para clientes, brochuras, software de demonstração e conjuntos de ações para download. Entre outros, o nosso catálogo "Safety Integrated".

Centro de informações e download (http://www.siemens.com/safety-infomaterial)

### Exemplos de funcionamento

Na Internet encontra práticos exemplos de funcionamento, que cobrem os requisitos típicos dentro da engenharia de segurança industrial. Obtém aplicações típicas com exemplos de produtos, incluindo esquema elétrico, código de programação e avaliação segundo EN 62061 e EN ISO 13849.

Exemplos de funcionamento na Internet (http://www.siemens.com/safety-functional-examples)

## Newsletter Safety Integrated

Nossa Newsletter periódica fornece-lhe informações atuais sobre a engenharia de segurança.

Newsletter Safety Integrated (http://www.industry.siemens.com/newsletter)

## Assistência no local

A Siemens fornece suporte aos seus clientes em todo o mundo com serviços relativos ao produto, sistema e aplicação, durante todo o ciclo de vida de uma instalação. Desde o planejamento e desenvolvimento, passando pelo funcionamento, até à modernização, os clientes beneficiam igualmente através do serviço, dos conhecimentos abrangentes sobre a tecnologia e o produto e da competência setorial dos técnicos da Siemens.

Industry Services (http://www.siemens.com/industry-service)

## Configuradores

Combine produtos e sistemas de forma simples, com a ajuda de nossos configuradores.

## Industry Mall

Por último, encomendar On-line no Industry Mall – não poderia ser mais simples.

Industry Mall (http://www.siemens.com/industrymall/)

## Aconselhamento

Para responder às exigências crescentes na área da engenharia de segurança, a Siemens aposta na Siemens Solution Partner Automation selecionada, para além de seus próprios técnicos em segurança. Estas empresas parceiras altamente qualificadas oferecem aconselhamento profissional e suporte ativo para todos os aspetos de segurança relevantes de seus projetos de automatização.

Solution Partner Internet (http://www.siemens.com/automation/solutionpartner)

# Índice

## A



## B



## C



## D



## E

## O



## P



## R



## S



## T



## U



## V